



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

OPNAVINST 5510.60M ^{IN REPLY REFER TO:}

DNS-34

MAR 23 2009

OPNAV INSTRUCTION 5510.60M

From: Chief of Naval Operations

Subj: SECURITY REGULATIONS FOR OFFICES UNDER THE COGNIZANCE
OF THE CHIEF OF NAVAL OPERATIONS

- Ref:
- (a) Executive Order 12958, as amended 25 March 2003
 - (b) SECNAV M-5510.36, Department of the Navy Information Security Program (ISP) Manual
 - (c) SECNAV M-5510.30, Department of the Navy Personnel Security Program (PSP) Manual
 - (d) SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy
 - (e) OPNAVINST 5530.14D, Navy Physical Security and Law Enforcement
 - (f) USSAN 1-70, United States National Security Authority for NATO (USSAN) Instruction (Industrial Security) (NOTAL)
 - (g) DoD Directive 5210.2, Access to and Dissemination of Restricted Data, 12 Jan 1978
 - (h) SECNAVINST 5720.42F, Department of Navy Freedom of Information Act Program
 - (i) CNO ltr 5510 N09N2/8U223000 of 7 Jan 2008, Subj: Updated Policy for "Declassify On" Markings (NOTAL)
 - (j) OPNAVINST 5513.1F, Department of the Navy Security Classification Guides
 - (k) DoD Manual 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006
 - (l) SECNAV M-5210.1, Department of the Navy Records Management Program, November 2007
 - (m) OPNAVINST 5511.35L, Safeguarding Nuclear Command and Control Extremely Sensitive Information
 - (n) SECNAVINST S5460.3F, Management, Administration, Support, and Oversight of Special Access Programs Within the Department of the Navy (U)
 - (o) NAVSEAINST 5511.32C, Safeguarding of Naval Nuclear Propulsion Information (NOTAL)
 - (p) SECNAVINST 5720.44B, Department of the Navy Public Affairs Policy and Regulations
 - (q) SECNAVINST 5510.34A, Disclosure of Classified

MAR 23 2009

Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives

- (r) Naval Information Assurance Publication, IA Pub-5239-22, Oct 2003
- (s) SECNAVINST S8126.1, Naval Nuclear Weapons Security Policy (NOTAL)
- (t) DoD Instruction 5200.33, Defense Courier Service Program, 19 May 07
- (u) OPNAVINST C5510.159, Guidelines Applicable to Communist Nationals Entering the United States as Non-Immigrant Aliens
- (v) Navy Telecommunications Directive (NTD) 09-6, Use of Portable Storage Devices, 6 Oct 06

Encl: (1) OPNAV Security Regulations

1. Purpose. To update security policy and procedural guidance for the protection of classified information and materials in the custody of the Chief of Naval Operations (CNO), the Office of the Chief of Naval Operations (OPNAV) staff or other Metro Washington, DC, Department of the Navy (DON) offices for which the CNO has cognizance for security. For the purpose of this instruction, offices under CNO cognizance are described as "OPNAV security serviced activities" as indicated at appendix A. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. OPNAVINST 5510.60L.

3. Objective. To ensure maximum uniformity and effectiveness in the application of the information, industrial, physical and personnel security program policies by the OPNAV security serviced activities.

4. Scope. This instruction is the basic guidance for the information, industrial, physical and personnel security programs for both military, civilian personnel, and supporting contractors as delineated by reference (a) and as assigned to DON under CNO's direction. By Memorandum of Agreement (MOA) between CNO and the Secretary of the Navy (SECNAV), the CNO provides policy and guidance for the protection of classified information and materials in the custody of those personnel

MAR 23 2009

assigned to the Navy in the Pentagon and temporary swing spaces throughout Metro-Washington, D.C. This instruction supplements references (b) and (c).

5. Action. All personnel assigned to OPNAV security serviced activities shall comply with references (b) through (k) and this instruction. Assistant For Administration, Under Secretary of the Navy/Office of Processing, Technology and Information (AAUSN/OPTI), in coordination with the OPNAV Command Information Office (CIO) (OPNAV (DNS-4)), will administer the Information Assurance (IA) Program for the OPNAV security serviced activities in accordance with reference (d) and chapter 18 of enclosure (1) of this instruction.

6. Violations of This Instruction

a. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this instruction.

b. Civilian employees are subject to criminal penalties under applicable Federal Statutes, a well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this instruction.

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with reference (1).

8. Reports and Forms

a. Reports. The reports identified in chapter 1 (paragraphs 3, 4 and 5), chapter 2, exhibit 7C (paragraph 5), and chapter 16 (paragraphs 1 and 2) of enclosure (1) of this instruction are exempt from reports control by SECNAV M-5214.1. Report control symbols OPNAV 5510-6B and OPNAV 5510-6C are required per reference (b), appendix C and as delineated in chapter 12 (subparagraph 7h) and chapter 16 (paragraph 1) of enclosure (1) of this instruction.

MAR 23 2009

b. Forms

(1) The following Standard Forms (SF) and Optional Forms (OF) can be downloaded from the General Service Administration (GSA) Forms Web site:

<http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?formType=SF>

- (a) OF 7 Property Pass
- (b) SF 153 COMSEC Material Report
- (c) SF 311 Agency Security Classification Management Program Data
- (d) SF 312 Classified Information Non Disclosure Agreement
- (e) SF 700 Security Container Information
- (f) SF 702 Security Container Check Sheet
- (g) SF 703 Top Secret (Coversheet)
- (h) SF 704 Secret (Coversheet)
- (i) SF 705 Confidential (Coversheet)

(2) The following SFs can be ordered through the Federal Supply System:

(a) SF 87A Finger Print Chart Stock Number (S/N)
7540-01-269-3384

(b) SF 701 Activity Security Checklist S/N 7540-01-
214-5372

(3) The following Department of Defense Forms (DD) can be downloaded from the DoD Forms Web site:

<http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>

(a) DD 254 Department of Defense Contract Security Classification Specification

(b) DD 1540 Registration for Scientific and
Technical Information Services

(c) DD 2345 Military Critical Technical Data
Agreement

(4) The following DD and OPNAV forms can be obtained
either from Naval Forms Online
<https://navalforms.daps.dla.mil/web/public/home> or the OPNAV
Security Office at the Pentagon, Room 5B542:

(a) DD 2501 Courier Authorization S/N 0102-LF-000-
6900

(b) DD 2918 Position Description

(c) OPNAV 5216/4 Outgoing Mail Record

(d) OPNAV 5239/14 System Authorization Access
Request Navy (SAAR-N)

(e) OPNAV 5239/15 Classified Hard Drive Destruction
Log

(f) OPNAV 5511/5 Security Violation Report

(g) OPNAV 5511/10 Record of Receipt S/N 0107-LF-008-
8000

(h) OPNAV 5511/12 Classified Material Destruction
Report

(i) OPNAV 5511/13 Disclosure Record (available in
Room 5B542)

(j) OPNAV 5511/14 Security Termination Statement

(k) OPNAV 5521/27 Visit Request

(5) The following forms are controlled and issued by
Pentagon Force Protection Agency (PFPA):

(a) DD 1199 Pentagon Reservation Parking Permit

MAR 23 2009

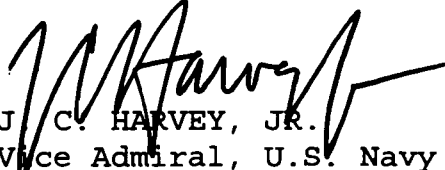
(b) DD 1466 Building Pass

(c) DD 2249 DoD Building Pass Application Control

(6) DOE HQ F 5631.20 Request For Visit or Access

Approval is available online at DOE via:

<http://www.directives.doe.gov/pdfs/forms/5631-20.pdf>



J. C. HARVEY, JR.
Vice Admiral, U.S. Navy
Director, Navy Staff

Distribution:

Electronic only, via Department of the Navy Issuances Web site

<http://doni.daps.dla.mil>

MAR 23 2009

OPNAV SECURITY REGULATIONS

MAR 23 2009

RECORD OF CHANGES

Identification of correction or change	date of change	date of entry	entered by
--	----------------	---------------	------------

MAR 23 2009

TABLE OF CONTENTS

IDENTIFICATION	TITLE	PAGE
CHAPTER 1	GENERAL REGULATION AND ORGANIZATION	
1.	Purpose.....	1-1
2.	Command Responsibility and Authority...	1-1
3.	Security Organization and Responsibilities.....	1-2
4.	Requests for Investigative Assistance..	1-9
5.	Counterintelligence Matters to be Reported.....	1-10
6.	Emergency Plan.....	1-12
7.	Security Education.....	1-13
8.	Debriefings.....	1-19
9.	Continuing Security Awareness.....	1-21
10.	Waivers.....	1-21
	Exhibit 1A.....	1A-1
	Exhibit 1B.....	1B-1
	Exhibit 1C.....	1C-1
CHAPTER 2	PERSONNEL SECURITY	
1.	Basic Policy.....	2-1
2.	Request for Clearance and Access.....	2-4
3.	Emergency Appointment to Sensitive Positions for Civilians.....	2-6
4.	Classified Information Nondisclosure Agreements.....	2-7
5.	Continuous Evaluation of Eligibility...	2-8
6.	Administrative Withdrawal of Adjudication of Clearance.....	2-9
7.	Denial or Revocation of Clearance/ Access for Cause.....	2-9
8.	Suspension of Access.....	2-10
9.	Clearances under DoD Industrial Security Program.....	2-11
10.	Access to CNWDI.....	2-11
11.	Debriefings.....	2-11
	Exhibit 2A.....	2A-1
	Exhibit 2B.....	2B-1
	Exhibit 2C.....	2C-1
	Exhibit 2D.....	2D-1
	Exhibit 2E.....	2E-1
	Exhibit 2F.....	2F-1

MAR 28 2000

	Exhibit 2G.....	2G-1
CHAPTER 3	BUILDING BADGES, PROPERTY PASSES AND CONTROL ACCESS CARD (CAC) ISSUANCE	
1.	DoD Building Passes.....	3-1
2.	Procedures for Badge Issuance.....	3-4
3.	Property Passes.....	3-6
4.	Contractor Verification System (CVS)...	3-7
CHAPTER 4	CLASSIFICATION	
1.	Basic Policy.....	4-1
2.	Classification Designations.....	4-1
3.	For Official Use Only (FOUO).....	4-2
4.	Original Classification Authority.....	4-3
5.	Original and Derivative Classification.	4-4
6.	Security Classification Guide.....	4-5
7.	Industrial Operations.....	4-6
CHAPTER 5	MARKING	
1.	Basic Policy.....	5-1
2.	Basic Marking Requirements.....	5-2
3.	Specific Marking Requirements for IT and Electronic Media.....	5-4
4.	Working Paper Marking.....	5-5
CHAPTER 6	HAND CARRYING OF CLASSIFIED MATERIAL	
1.	Within a Command or Immediate Environs.	6-1
2.	Procedures for Acquisition and Use of Courier Authorization Cards.....	6-1
3.	Authorization to Hand Carry Classified Material in a Travel Status.....	6-2
4.	Protection During Hand Carrying in a Travel Status.....	6-2
5.	Procedures for Obtaining Authorization to Escort or Hand Carry Classified Material on Commercial Passenger Aircraft.....	6-3
6.	Procedures for Carrying Classified Documents Aboard Commercial Passenger Aircraft.....	6-4
	Exhibit 6A.....	6A-1
	Exhibit 6B.....	6B-1

[MAR 28 2000]

CHAPTER 7	ACCOUNTING AND CONTROL	
1.	Basic Policy.....	7-1
2.	Top Secret.....	7-1
3.	Secret.....	7-3
4.	Confidential.....	7-4
5.	Secret and Confidential Working Papers.	7-5
6.	Top Secret Working Papers.....	7-5
7.	Special Types of Classified and Controlled Information.....	7-5
	Exhibit 7A.....	7A-1
	Exhibit 7B.....	7B-1
	Exhibit 7C.....	7C-1
CHAPTER 8	PRINTING REPRODUCTION AND PHOTOGRAPHY	
1.	Controls on Reproduction.....	8-1
2.	Tele copiers.....	8-3
3.	Requirement for Photography and Imaging Technology in Pentagon and Related NCR Facilities.....	8-3
	Exhibit 8A.....	8A-1
CHAPTER 9	DISSEMINATION OF CLASSIFIED MATERIAL	
1.	Basic Policy.....	9-1
2.	NATO Material.....	9-1
3.	Top Secret Material.....	9-1
4.	Secret and Confidential Material.....	9-2
5.	Dissemination of DoD Contractors.....	9-2
6.	Disclosure to Foreign Government and International Organizations.....	9-2
7.	Dissemination to Congress.....	9-2
8.	General Policy for Dissemination of Intelligence.....	9-2
9.	Procedures for the Release of Intelligence to Contractors.....	9-4
10.	Sanitization.....	9-4
11.	Prohibited Release.....	9-4
CHAPTER 10	TRANSMISSION OF CLASSIFIED MATERIAL	
1.	Basic Policy.....	10-1
2.	Top Secret.....	10-1
3.	Secret.....	10-2
4.	Confidential.....	10-4
5.	Telephone Transmission.....	10-5

[MAY 28 2000]

6.	Receipt Systems.....	10-5
7.	Transmission to Foreign Governments....	10-6
8.	Transmission of COMSEC Material.....	10-6
9.	Transmission of RD.....	10-6
10.	Transmission of SCI.....	10-6
11.	Transmission of SAP.....	10-6
12.	Transmission of NC2-ESI.....	10-6
13.	Transmission of FOUO and SBU.....	10-6
14.	Consignor-Consignee Responsibility....	10-6
15.	Classified Material Preparation for Transmission.....	10-6
16.	Addressing of Classified Material.....	10-6
17.	DCS.....	10-8
CHAPTER 11	SAFEGUARDING AND SECURITY STORAGE	
1.	Responsibility for Safeguarding.....	11-1
2.	Security Containers.....	11-2
3.	Combinations.....	11-4
4.	Locking Procedures.....	11-5
5.	OPNAV Locksmith Services.....	11-5
6.	Areas Protected by Electronic Alarm Systems.....	11-5
7.	Opening and Securing Alarm Areas.....	11-7
8.	Unalarmed Work Spaces.....	11-7
9.	Care of Working Spaces.....	11-8
10.	Security Check Lists.....	11-8
11.	Key and Lock Control.....	11-9
	Exhibit 11A.....	11A-1
CHAPTER 12	DESTRUCTION OF CLASSIFIED MATERIALS	
1.	General.....	12-1
2.	Procedures.....	12-1
3.	Destruction Report.....	12-2
4.	Message Traffic.....	12-2
5.	Destruction of CMS Material.....	12-3
6.	Emergency Action Procedures.....	12-3
CHAPTER 13	OPNAV SECURITY SERVICES	
1.	Pentagon Parking Program.....	13-1
2.	Authority.....	13-1
3.	Responsibilities.....	13-1
4.	Assignment of Parking Permits.....	13-2
5.	Physically Disabled Parking.....	13-2
6.	Visitor Parking.....	13-3

[MAR 28 2000]

7.	Car Pool Parking.....	13-3
8.	Parking Regulations.....	13-4
9.	DD 2501 Courier Cards.....	13-5
10.	Fingerprinting Procedures.....	13-5

CHAPTER 14 VISITS AND MEETINGS

1.	General.....	14-1
2.	Outgoing Visits.....	14-1
3.	Incoming Visits.....	14-2
4.	Visits to DOE Activities.....	14-3
5.	Visits by Representatives of the Government Accountability Office (GAO).....	14-3
6.	Visits by Foreign Nationals.....	14-3
7.	Classified Meetings.....	14-4
8.	Unclassified Meetings.....	14-5

CHAPTER 15 INDUSTRIAL SECURITY

1.	General.....	15-1
2.	Classified Contracts.....	15-1
3.	Contract Security Classification Specification (DD 254).....	15-1
4.	Classified Visits to OPNAV Security Serviced Activities by Contractor Personnel.....	15-2
5.	Dissemination of Classified Material to DoD Contractors.....	15-3
6.	Procedures for Issuance of DoD Building Passes to Contractor Personnel.....	15-4
7.	Consultant Clearances.....	15-4
	Exhibit 15A.....	15A-1
	Exhibit 15B.....	15B-1

CHAPTER 16 COMPROMISE AND OTHER VIOLATIONS

1.	General.....	16-1
2.	Security Violations.....	16-2
3.	Administrative Sanctions, Civil, Remedies and Punitive Actions.....	16-6
4.	Review of Violation Reports.....	16-7

CHAPTER 17 FORCE PROTECTION MEASURING AND PLANNING

1.	Introduction.....	17-1
2.	Responsibilities.....	17-1
3.	Force Protection Conditions (FPCONS)...	17-1

MAR 23 2003

CHAPTER 18	INFORMATION SYSTEM (IS) SECURITIES	
1.	Purpose.....	18-1
2.	E-Ring Activities.....	18-1
3.	Command Responsibility and Authority...	18-1
4.	User Role and Responsibilities.....	18-1
5.	OPNAV Outlook Web Access (OWA) Requirements.....	18-4
6.	Portable Computer Devices Requirements.	18-5
	Exhibit 18A.....	18A-1
CHAPTER 19	EMERGENCY PROCEDURES AND NOTIFICATIONS	
1.	Purpose.....	19-1
2.	Procedures.....	19-1
3.	Notifications.....	19-3
APPENDIX A	OPNAV SECURITY SERVICED ACTIVITIES' UICs	A-1

MAR 23 2003

CHAPTER 1
GENERAL REGULATIONS AND ORGANIZATIONS

1. Purpose

a. This instruction establishes uniform security policies for OPNAV security serviced activities under the cognizance of the OPNAV Security Office (OPNAV (DNS-34)). It delineates responsibilities and procedures to ensure that information classified under the authority of reference (b) is protected from unauthorized disclosure. It ensures that appointment or retention of civilian employees of the command, acceptance or retention of military personnel in the command, granting access to classified information or assignment to other sensitive duties, is clearly consistent with the interest of national security and the policies established in references (b) through (k). In the absence of specific reference to requirements here or in other separate directives, the provisions of references (b) through (k) apply.

b. This instruction does not apply to the handling and management of Sensitive Compartmented Information (SCI).

2. Command Responsibility and Authority

a. The Director Navy Staff (CNO (DNS)) is designated to administer information, industrial and security education and training, physical and personnel security, and the mandatory declassification review programs for the OPNAV security serviced activities.

b. The CNO (DNS) will be assisted by the Director of Management (OPNAV (DNS-3)) in security administration and enforcement of the above security programs.

c. The head of OPNAV (DNS-34) is responsible for the formulation, implementation and enforcement of security programs, their effectiveness and compliance with all the directives issued by higher authority. OPNAV (DNS-34) is concurrently designated as the OPNAV security manager under the provisions of references (b) and (c) and security officer under the provisions of reference (e). As a tenant office for physical security and law enforcement purposes under the auspices of PFPA, regular communications with PFPA's Communications and Operations Division are essential, and feedback from the monthly Pentagon Security Advisory Group (PSAG) meetings is required.

MAR 28 2003

3. Security Organization and Responsibilities

a. The OPNAV Security Manager (OPNAV (DNS-34))

(1) OPNAV (DNS-34) is the principal advisor for information, industrial, security education and training, physical and personnel security program policies within the command. The security manager is responsible to CNO (DNS) for the management, formulation, implementation and enforcement of security policies and procedures for the protection of classified information originated by and/or under the cognizance of CNO, and by MOA, the immediate offices of SECNAV and DON staff offices. In connection with the duties outlined in references (b) through (k), and to monitor command compliance, disclosure of classified information is authorized, and access to all areas shall be given to appropriately identified representatives of OPNAV (DNS-34) during the conduct of assigned duties to include investigations, inspections and security assist visits.

(2) Concurrently OPNAV (DNS-34) serves as the umbrella for security direction, guidance and policy for all OPNAV security serviced activities via assigned security coordinators. Appropriate departmental security matters are also coordinated with Headquarters Marine Corps (HQMC) Security Branch.

b. Security Inspections and Security Assist Visits

(1) Formal security inspections are not mandatory by higher directives but will be conducted for each OPNAV security serviced activity as deemed necessary by OPNAV (DNS-34) to review compliance with the requirements of this instruction and to examine overall security postures in accordance with references (b) through (k). When security inspections are done, a formal report shall be generated and forwarded by OPNAV (DNS-34) to the OPNAV security serviced activity's deputy or executive assistant. Identified deficiencies will be marked as requiring action with a formal written reply from the OPNAV security serviced activity to CNO (DNS) via OPNAV (DNS-34) covering specific correction of any deficiencies. If required by inspection results, a re-inspection will be conducted by OPNAV (DNS-34).

(2) Security assist visits will be conducted by the OPNAV's security inspection team under the guidance of OPNAV (DNS-34) upon request by a designated security coordinator.

MAR 23 2003

Security assist visits will be accomplished in an informal manner and may cover all security requirements or specific items as desired by the requesting security coordinator. The purpose of the security assist visit is to provide assistance in achieving security requirements prior to a formal inspection. It is not an inspection of compliance with security policy.

c. OPNAV (DNS-34) is assisted in the performance of assigned duties by the staff listed below:

(1) Head, Personnel Security (OPNAV (DNS-34B)), is responsible for:

(a) The development, implementation and monitoring of the Personnel Security Program to include the approval and initiation of required investigations for personnel security clearances, the granting of classified access, the review of investigative reports to determine the necessity for further information, and the pre-employment check of proposed civilian personnel.

(b) Ensuring that all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for Personnel Security Investigations (PSIs) are properly prepared, submitted and monitored.

(c) Ensuring that access to classified information is limited to those with the need to know.

(d) Ensuring that PSIs, clearances and access are recorded.

(e) Managing the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(f) Maintaining liaison with the command Special Security Officer (OPNAV (N21)) concerning investigations, access to SCI, continuous evaluation of eligibility, and changes to information and personnel security policies and procedures.

(2) Head, North Atlantic Treaty organization (NATO) Sub-registry Section (OPNAV (DNS-34C)), is responsible for the development and implementation of the NATO/Treaty Material Security Program for those offices, commands and agencies

MAR 23 2000

serviced by the OPNAV (DNS-34C). For Central U.S. Registry customer support, refer to <https://secureweb.hqda.pentagon.mil/cusr>.

(3) Head, Information Security/Security Education Section (OPNAV (DNS-34D)), is responsible for:

(a) The development and monitoring of an information security program to include classification management, coordination of the preparation and maintenance of classification guides issued by the command, and ensuring compliance with accounting and control requirements for classified material.

(b) The development and monitoring of an industrial security program to encompass the processing of personnel clearances/facility clearances/storage capability for unpaid consultants; including designated "contracting officer's representative" for classified contracts with Department of Defense (DoD) contractors, and, as such, has signature authority on legal contractual documents (DD 254 Department of Defense Contract Security Classification) for such contracts, and authorizes requests for facility clearance/storage capability for contractor facilities.

(c) The development and implementation of the Security Education and Training Program to include conducting security briefings for command personnel, obtaining outside training when and where required, and approving and monitoring training provided by security coordinators for personnel under their cognizance.

(d) The development and implementation of a command security awareness program. Develops and disseminates newsletters, flyers, posters and other media/materials to enhance the security awareness of all command personnel.

(e) Maintaining records of personal/official foreign travel reported by command personnel.

(f) The development and implementation of a security assist visit program to provide oversight and assistance on compliance with security requirements by OPNAV security serviced activities. Scheduling and conducting assist visits when requested by security coordinators, and providing oral/written reports on findings and recommendations.

MAR 23 2000

(g) Maintaining liaison with the command OPNAV (N21) concerning investigations, access to SCI and continuous evaluation of eligibility for personnel and facilities under the DoD Industrial Security Program.

(h) Ensuring security control of visits to the command when the visitor requires, and is authorized access to classified information.

(i) Ensure compliance of the OPNAV security serviced activities with DON and command security policies and procedures.

(4) The OPNAV CIO (OPNAV (DNS-4)):

(a) Is designated as the CIO, the Telecommunications Electro-Magnetic Protection, Equipments, Standards and Techniques (TEMPEST) control officer, and is responsible for the computer security and IA for each OPNAV security serviced activity.

(b) Ensures that Assistant Contract Technical Representatives (ACTRs) are properly designated for each OPNAV security serviced activities as required.

(c) Provides policy and procedural guidance to the ACTRs and others involved with Information Technology (IT) security matters.

(d) Reviews and recommends action on requests for interim authority to operate and authority to operate accreditation, and other IT security and documentation as required.

(5) Head, Department of the Navy Mail Center, Facility Services Division, AAUSN, will assist with the requirement for classification management by reviewing all outgoing classified documents for appropriate classification markings, including page, paragraph/portion and downgrading/declassification statement. Ensure that all outgoing classified material to contractor facilities contains the information and certification required by chapters 9 and 15.

(6) OPNAV (DNS-34C) will disseminate all Nuclear Command and Control Extremely Sensitive Information (NC2-ESI) material to the Deputy Chief of Naval Operations (Operations, Plans and

[NO 20 2000]

Strategy) (CNO (N3/N5)) NC2-ESI control officer only. Further dissemination of NC2-ESI material will be determined and accomplished by the NC2-ESI control officer.

d. Each OPNAV security serviced activity must:

(1) Appoint an individual in writing to serve as the security coordinator for their organizational entity (see exhibit 1A for sample letter). Security coordinators will serve in their appointed capacity until relieved. Assistant Security Coordinators (ASCs) may be appointed if required to assist the security coordinator in performance of his/her duties (see exhibit 1B for ASC sample letter). However, ultimate responsibility for command's security programs still resides with the security coordinator.

(a) Security coordinators will assist in implementing the security programs by:

1. Ensuring all personnel under their cognizance comply with security regulations.

2. Serving as a communication link between OPNAV (DNS-34) and personnel under their cognizance.

3. Continually monitoring control measures (document, physical, etc.) for effective operation.

4. Conducting annual security refresher briefings to personnel under their cognizance.

5. Forwarding visit requests via Joint Personnel Adjudication System (JPAS) to outside activities for personnel under their cognizance.

6. Nominating personnel under their cognizance for DD 2501 Courier Authorization Cards as required by billet sensitivity.

7. Reviewing classified material prepared in their organization for correct classification and marking.

8. Promoting security consciousness within their organization in support of the command security awareness program.

[MAR 28 2000]

9. Ensuring that all assigned personnel have a personnel security clearance/access according to the billet sensitivity.

10. Establishing visitor control procedures within command to preclude unauthorized access to spaces containing classified information.

11. Investigating security violations.

12. Ensuring all assigned personnel attend required security education training.

13. Ensuring compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

14. Briefing new personnel on local security practices within 1 week of their assignment and providing the employee with a copy of the local security instruction.

15. Coordinating IA issues with the OPNAV Command Information Assurance Manager (IAM) (OPNAV (DNS-44)).

16. Annually self-inspecting the offices under their cognizance, using the checklist contained in chapter 2, exhibit 2C of reference (b) and providing a copy to OPNAV (DNS-34) upon completion of the self-inspection.

(b) ASCs, designated in writing per exhibit 1B, are responsible for carrying out the following tasks:

1. Serve as a communication link between security coordinators and cognizance staff personnel.

2. Report security violations to respective security coordinators and OPNAV (DNS-34).

3. Ensure that personnel under their cognizance conform to the guidance of this instruction and report discrepancies to the security coordinator and the immediate supervisor.

4. Relay problems or items requiring clarification to security coordinators.

MAR 23 2009

5. Assist security coordinators with other security duties as required (i.e., distribution of security newsletters, security posters, promulgation of policy clarification, security education and training, etc.).

(c) Security coordinator/ASC may be assigned as a full-time, part-time or collateral duty, but the person designated must be an officer/enlisted E-6 or above or a civilian employee in career group YA (Professional/Analytical), YB (Technical/Support) or YC (Supervisor/Manager), with sufficient authority and staff to manage the program for the directorate. Assigned contractors may serve as an ASC with concurrence of OPNAV (DNS-34). The security coordinator should be afforded direct access to the OPNAV security serviced activity head. The security coordinator/ASC must be a U.S. citizen and have been the subject of a favorably adjudicated security investigation. OPNAV security serviced activity heads are strongly advised to only appoint individuals with previous experience in handling classified material and knowledge of DON security procedures.

(d) The usefulness of the Security Coordinator Program is contingent upon effective communication, training and two-way discussions with OPNAV security personnel. The program does not satisfy all requirements for implementing and maintaining a viable command security program. Instead, because of the size and complexity of the commands supported by OPNAV (DNS-34), it is designed to enhance security awareness, improve operational security practices and serves as a feedback mechanism for OPNAV (DNS-34).

(2) Designate the Top Secret Control Officer (TSCO) and, Assistant Top Secret Control Officers (ATSCOs), if required, in writing (per exhibit 1C), who will be responsible for the receipt, control, reproduction, destruction, transmission and inventory of all top secret material for the command. The TSCO will be subordinate to the security coordinator. ATSCOs may be appointed at the division level to assist the TSCO in performance of duties; the TSCO is still responsible for those duties and, with the designated alternate, are the only individuals authorized to receipt for top secret material. The person designated as the TSCO/ATSCO must be an officer, senior non-commissioned officer (E-7 or above) or a civilian employee in career group YA (Professional/Analytical), YB (Technical/Support) or YC (Supervisor/Manager). TSCO/ATSCO must be a U.S. citizen who has been the subject of a Single Scope Background Investigation (SSBI) within the past 5 years and is

MAR 23 2003

completely familiar with the requirements for protection of top secret information and the duties described in paragraph 2-3 of reference (b).

(3) Provide a copy of all letters of appointment for security coordinators, TSCOs and their ATSCO (including names, applicable code, location and telephone numbers) to OPNAV (DNS-34) and inform OPNAV (DNS-34) of changes as soon as they occur. These individuals shall interface directly with OPNAV (DNS-34) and are the focal point for their respective directorates on all applicable security matters.

(4) Issue command security procedures for offices under their cognizance in addition to those contained in references (b) and (c) and this instruction and submit to OPNAV (DNS-34) prior to implementation for review. Procedures must include, but will not be limited to, the following areas:

(a) Establish an accounting and control system for top secret and secret material to include destruction procedures.

(b) Assign responsibilities for review of classification and associated markings on documents to ensure accuracy and completeness.

(c) Notify all personnel of the location of classification guides and policy on the use of Original Classification Authority (OCA).

(d) Internal security training program.

(e) Implementation of an annual self-inspection program and clean out day for the purpose of reducing classified holdings.

4. Requests for Investigative Assistance

a. On behalf of CNO (DNS), OPNAV (DNS-34) liaises with the Naval Criminal Investigative Service (NCIS), Office of Personnel Management (OPM), Defense Security Services (DSS) and PFFA on matters of PSIs and civil or criminal investigative matters involving personnel from OPNAV security serviced activities, except as outlined in chapter 16, paragraph 2. Utilization of CNO (DNS) as the focal point for such matters is required to

MAR 23 2003

avoid delayed processing of cases and possible embarrassment to the Navy (e.g., improper channeling or dissemination of sensitive information).

b. OPNAV security serviced activities' security officers and supervisors will promptly report all incidents of actual, suspected or alleged criminal offenses to OPNAV (DNS-34). Investigative assistance, or other action as appropriate, will be promptly initiated to ensure expeditious resolution while protecting the interests of the Navy and the due process rights of the individual. OPNAV (DNS-34) will keep appropriate officials advised of pertinent developments as investigation, processing or other required administrative action proceeds.

5. Counterintelligence Matters to be Reported

a. Basic Policy. Certain matters affecting national security must be reported to NCIS so appropriate counterintelligence action can be taken. All OPNAV security serviced activities' personnel, whether they have access to classified information or not, will report to OPNAV (DNS-34) any activities described in this paragraph involving themselves, their dependents or others. OPNAV (DNS-34) will, in turn, notify NCIS.

b. Sabotage, Espionage or Deliberate Compromise

(1) Any individual becoming aware of possible acts of sabotage, espionage, deliberate compromise or other subversive activities will report all available information concerning such action immediately to OPNAV (DNS-34).

(2) All OPNAV security serviced activities' personnel will immediately notify OPNAV (DNS-34) of any requests, through other than official channels, for classified national defense information from anyone regardless of nationality, or for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, personal data or characterizations of DON personnel; technical orders, manuals, regulations, command directories or personnel rosters; and information about the designation, strength, mission, combat posture, and development of ships, aircraft and weapons systems.

[MAR 28 2003]

c. Contacts with Citizens of Foreign Countries

(1) Innocent contacts with citizens of foreign countries are not, in themselves, wrong, against regulations or illegal. All personnel will promptly report to OPNAV (DNS-34) for forwarding to NCIS any suspicious form of contact, intentional or unintentional, with any citizen, official, office, establishment or entity of a foreign country. NCIS will evaluate the contacts and take action to protect the DON from hostile intelligence activities. This is particularly so regarding contacts for information that suggest DoD personnel may be targeted. Report any attempt to exploit by a foreign intelligence source or international terrorist organization; contact with a known suspected intelligence officer from any country; contact with anyone receiving information of planned, attempted, actual, or suspected international terrorism, or other intelligence activities against the DoD facilities or U.S. citizens. Personnel will notify OPNAV (DNS-34) before contacting or visiting any establishment of a foreign country, including those located in the United States and friendly countries. Subsequent to the contact or visit, individuals must again report to OPNAV (DNS-34) for debriefing.

(2) For sensitive compartmented or special access billets, additional foreign national contact information may be required. Contact the Special Security Officer (CNO (SSO)) or Special Access Program Security Office for further details on all personal or professional non-U.S. citizen contacts, inside or outside the United States, in which continuous contact or confide personal information is maintained. This would include any non-U.S. citizen relative by blood or marriage who resides in the U.S. or overseas, including U.S. legal permanent resident's green card holders registered with Immigration and Naturalization Services.

(3) See also chapter 1, subparagraph 7(f), for information regarding foreign travel briefing requirement.

d. Suicide or Attempted Suicide. When any individual who had access to classified information commits or attempts suicide, the individual's security coordinator or supervisor will immediately forward all available information to OPNAV (DNS-34) for reporting to NCIS and the Special Assistant for Naval Investigative Matters and Security (CNO (N09N)). The report will, as a minimum, set forth the nature and extent of

[MAR 28 2003]

the classified information to which the individual had access and the circumstances surrounding the suicide or attempted suicide.

e. Unauthorized Absentees. When any individual who has access to classified information is in an unauthorized absentee status, the individual's security coordinator or supervisor will notify OPNAV (DNS-34) and conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that his/her absence may be inimical to the interests of national security. The results of this report will be submitted to OPNAV (DNS-34). If the inquiry reveals such indications, OPNAV (DNS-34) will report all available information to the NCIS for action.

f. Foreign Travel

(1) All OPNAV security serviced activities' personnel possessing a security clearance are required to report to OPNAV (DNS-34D) all personal foreign travel in advance of the travel being performed. Supervisors will keep this reporting requirement in mind when they are approving leave for their personnel and ensure individuals report to OPNAV (DNS-34D). Personnel will be reminded of this reporting requirement during orientation security briefings and annual refresher security briefings.

(2) For Out of Continental United States (OCONUS) travel, personnel must have attended a foreign travel briefing within 12 months. Briefings are provided by PFPA on the first Tuesday every month in the Pentagon Conference Center (PLC2) at 1200. Follow-up requirements may be completed on-line at www.at-awareness.org. All completed certificates will be forwarded to OPNAV (DNS-34) for record keeping.

(3) When travel patterns (i.e., numerous expensive trips abroad or very frequent travel) or the failure to report such travel indicate the need for investigation, OPNAV (DNS-34) will refer the matter to NCIS for action.

6. Emergency Plan

a. Emergency procedures for protecting or removing classified material in the event of natural disaster, civil disturbance or enemy action will be followed as outlined in subparagraphs 6b and 6c below.

MAR 28 2000

b. The Navy Continuity of Operations Plan (U) (SECNAVINST S3030.5 (NOTAL)) discusses pre-positioning duplicate records essential to continuity of operations during war/emergency situations. Essential records not pre-positioned may be hand-carried in accordance with references (b) and (c).

c. In case of evacuation due to fire or natural disaster, individuals in spaces accredited for open storage will evacuate according to the alarm and "Big Voice" announcements. The combination lock on door will be secured; do not set to alarm. For those personnel who have security containers only, put all classified working papers in security containers and lock them. Personnel safety is paramount. These procedures shall be implemented only when the personal safety of individuals is not in jeopardy. PFFA, along with Navy security augmenters, will provide perimeter protection of areas involved.

7. Security Education

a. Basic Policy. DON policy requires that all commands which handle classified information establish and maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures. The CNO (N09N) Web site, <http://www.navysecurity.navy.mil>, provides supporting education policy and related links for Defense Security Program reference.

b. Purpose of the Program

(1) The Security Education Program instills an appreciation of the need for protecting classified information from hostile threats, what those threats are and ways used by the threats to obtain classified information. The Information and Personnel Security Programs provide a framework for protection of information and controlled dissemination that are essential to national security. In an open society, such as that of the United States, disclosure outside authorized channels is tantamount to disclosure to a hostile intelligence service.

(2) The purpose of the Security Education Program is to make sure that all personnel understand the need to protect classified information and know how it is to be safeguarded. The goal is to develop fundamental habits of security to the

MAR 28 2000

point that proper discretion is automatically exercised in the discharge of duties and security of classified information becomes a natural element of every task.

c. Responsibility

(1) OPNAV (DNS-34D) is responsible for administering the Security Education Program via security coordinators and their assistants. Two mandatory semi-annual training sessions will take place for the purpose of satisfying security coordinator's training. OPNAV (DNS-34) will assist security coordinators in obtaining training materials and training aids; the security coordinators will conduct initial orientation and annual training for personnel under their cognizance. Duties and security topics are discussed further below.

(2) Supervisors and security coordinators are responsible for two security education functions:

(a) Identifying security requirements applicable to their organizational elements.

(b) Ensuring that personnel under their supervision understand and comply with the security requirements for their particular assignments.

d. Scope. Security education will be available to all command personnel including contractors, reservists and those assigned on temporary duty (including assigned HQMC personnel) from other Government agencies, whether or not they have access to classified information. More extensive training will be provided for members who have access to classified information. Records will be maintained in the command's security database, OPNAV Automatic Security Information System (OASIS).

e. Minimum Requirements

(1) Indoctrination

(a) Everyone who enters the Department of the Navy for service will have a basic understanding of what classified information is, and why and how it is protected.

(b) Normally this basic indoctrination is done during training at the time of accession. However, since past experience has proven that new personnel are not usually provided indoctrination training prior to reporting aboard the

MAR 28 2000

command and no record is available for OPNAV (DNS-34) to verify any prior security indoctrination, all new personnel will receive security indoctrination as a part of their check-in process with their respective security coordinator. This will afford the security coordinator an opportunity to emphasize specific security information required by the individual pertaining to his/her duties and physical office location, familiarize the individual with his/her security coordinator for future use and eliminate the employee from having to report for numerous check-in type meetings.

(c) A written security indoctrination briefing stating basic security requirements will be given to each employee by OPNAV (DNS-34) on the day of check-in as prerequisite to getting the building badge. In addition, within 1 week, the security coordinator must brief the employee on basic principles of security and local security procedures within their respective directorate/division and must certify that the briefing has been accomplished by countersigning the OPNAV 5510/418 Security Indoctrination Certification and Request for Clearance and Special Access form provided by the security office at check-in. Indoctrination and orientation training may be satisfied by way of bi-monthly OPNAV (DNS-34) security refresher briefings.

(d) As a minimum, the indoctrination training will include sufficient information to make the individual aware that:

1. Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;
2. Classified material will be marked to show the level of classification (top secret, secret or confidential);
3. Classifiable information is information which should have been marked as classified, but which, as a result of negligence, time constraints, error, lack of opportunity or oversight, has not been marked as classified;
4. Only those who have been officially and specifically authorized may have access to classified information;

(17) 2 0 2000

5. Classified material must be stored and used in security areas, protected during transfer from one area (or OPNAV security serviced activity) to another, and destroyed by authorized means;

6. Any breach of security must be reported to their security coordinator or OPNAV (DNS-34);

7. Any contact with a foreign national that binds the member to that foreign national by affection or obligation, shall be reported as soon as the member realizes obligation has occurred; and

8. Any attempt by an unauthorized person to solicit classified information must be reported to their security coordinator or OPNAV (DNS-34).

(2) Orientation

(a) Each person who will have access to classified information will be given an orientation briefing as soon as possible after reporting aboard or being assigned to duties involving classified access.

(b) OPNAV (DNS-34) will present bi-monthly scheduled command orientation briefings. Personnel will be scheduled for orientation briefings as part of their check-in with OPNAV (DNS-34).

(3) On-The-Job Training

(a) Supervisors are responsible for training employees on security requirements and the specific impact upon their duties. On-the-job training is the phase of security education when application of specific security procedures is learned.

(b) Supervision of the on-the-job training process is critical. Leaving subordinates to learn by trial-and-error is costly to security, as is assuming they know how classified information is to be protected. In reviewing compromise/violation reports, it is often found that fault lay with the supervisor who assumed that subordinates knew what they were supposed to do. Examples include:

(M 20 00)

1. Assigning duties as "accounting and control clerk," particularly as a substitute without instruction on proper accounting and receipt procedures;

2. Assigning responsibilities for mailing classified material without training in the preparation and transmission of classified material;

3. Designating top secret control duties without reviewing control requirements;

4. Assigning responsibility for originating classified information without training in proper classification procedures;

5. Not referencing Security Classification Guides (SCGs) nor having guides available within the office; and

6. Assigning typing duties for classified material without instruction on what constitutes security, what classification markings are, and lack of training on the placement of classification markings on typed documents.

(4) Annual Refresher Briefing

(a) At least once a year, OPNAV security serviced activities' personnel will receive a refresher briefing covering the following issues:

1. Recent counterintelligence highlights;
 2. Examples of common security violations;
 3. Procedural changes;
 4. Terrorism - Anti-Terrorism Force Protection;
- and
5. Reporting requirements.

(b) The refresher briefing does not have to cover the whole subject of security. Since it is unlikely to schedule everyone in the command at the same time, the refresher briefing will be more effective if it is tailored for a particular group. For example, the briefing should include guidance on policy and procedural changes, plus required counterintelligence reminders. For clerical personnel, concentrate on the preparation of

MAR 23 2003

classified material, or for those who draft classified documents, review the procedures for classifying and marking material. A review of the requirements governing hand-carrying classified material would be appropriate for those who are most likely to travel on command business. A review of clearance criteria and adjudicative policy would be appropriate for supervisors of cleared personnel.

(c) Security coordinators will either schedule participants at the bi-monthly refresher briefing by OPNAV (DNS-34) or provide the briefing personally and notifying OPNAV (DNS-34D) in writing of the full names and briefing date of those attended.

(5) Counterintelligence Briefing. Attendance is required annually for those who have access to information classified at the secret level or above. The counterintelligence briefing is also required annually for members with SCI clearances. The briefing is conducted by an NCIS agent and is designed to enhance awareness of personnel to the hostile intelligence and terrorist threat. OPNAV (DNS-34D) will routinely coordinate with NCIS and arrange counterintelligence briefings.

f. Special Briefings. The below special briefings must be attended as follows:

(1) Foreign Travel Briefing

(a) Any individual who has had access to classified information and who plans to travel OCONUS on official business or while on leave shall report these plans to his/her security coordinator, who must schedule a force protection briefing with PFPA. This includes individuals intending cruises.

(b) Personnel will be made aware of foreign travel briefing requirements by their security coordinator with other required security training.

(c) When the individual returns with specific reportable information, he/she must be debriefed by OPNAV (DNS-34) to provide the opportunity to report any incident - no matter how insignificant it might have seemed - that could have security implications. OPNAV (DNS-34) will maintain record of the brief and debrief for follow-up.

MAR 23 2000

(d) The foreign travel briefing is only required for those who have had access to classified information but it may be given to dependents, or others without access, upon request of command sponsor. Briefings to dependents, or others without access, will be unclassified.

(2) NATO Briefings. All personnel who require access to NATO information must be briefed in accordance with reference (f) on NATO security procedures before access may be granted. This briefing is given by OPNAV (DNS-34C) or the NATO control points approved and briefed by OPNAV (DNS-34C). Personnel receiving the NATO briefing for the purpose of Secure Internet Protocol Router Network (SIPRNET) accreditation will not be granted NATO access.

(3) NC2-ESI. A special briefing is required before access to NC2-ESI may be granted. An SF 312 Classified Information Nondisclosure Agreement and debriefing certificate, as required by paragraph 4-11 of reference (c) must be executed. This briefing (and debriefing) is given by CNO (N3N5) (NC2-ESI control officer).

(4) SCI. OPNAV (N21) is responsible for access and billets for SCI. In that capacity, OPNAV (N21) will initiate investigations and update JPAS access, as well as provide documentation to OPNAV (DNS-34) for the purpose of granting general service clearances.

(5) Critical Nuclear Weapons Design Information (CNWDI). Refer to reference (g), for information concerning the briefing/debriefing requirements for access to CNWDI.

8. Debriefings

a. Security coordinators/ASCs under the following conditions must debrief those personnel who have had access to classified information:

(1) Prior to termination of active military service or civilian employment including retirement, terminal leave periods when member is not returning to the command, or temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.

(2) At the conclusion of the access period, when a Limited Access Authorization has been granted.

MAR 23 2003

(3) When security clearance is revoked.

(4) When security clearance access is administratively withdrawn.

b. A debriefing will also be given, and an OPNAV 5511/14, Security Termination Statement, executed, when a member of the command inadvertently has substantive access to information which he or she is not eligible to receive.

c. At the debriefing, security coordinator or designated assistant will make clear to the individual that all classified material in his or her possession must be returned; that he or she may never divulge classified information, orally or in writing, to any unauthorized person or in judicial, quasi-judicial, or administrative proceedings and that there are severe penalties for disclosure; and that he/she must report to NCIS (or to the Federal Bureau of Investigation (FBI) or nearest DoD component, if no longer affiliated with DON), without delay, any attempt by an unauthorized person to solicit classified information. If possible, will remind the individual of the kinds of classified briefer information to which he/she had access.

d. The individual will then be required to read the provisions of the Espionage Act and read and sign OPNAV 5511/14. The witness to the signature then signs OPNAV 5511/14. If an individual refuses to execute an OPNAV 5511/14, the briefer will ensure the individual is debriefed and stress the fact that refusal to sign does not change the obligation to protect classified information from unauthorized disclosure. Briefer will annotate the statement to show that the individual refused to sign and send a copy to OPNAV (DNS-34).

e. The Office of the Secretary of Defense (OSD) has specifically directed that OPNAV 5511/14s shall be executed by senior officials (flag and general officers, ES-1 and above, Senior Executive Service (SES) and equivalent positions). The immediate senior of the senior official will ensure that the statement is executed and that failure to execute the statement is reported immediately to the Deputy Under Secretary of Defense for Policy via Deputy Assistant Secretary of Defense for Security and Information Operations via OPNAV Security Policy Branch (OPNAV (N09N2)).

f. The original OPNAV 5511/14 will be placed in the individual's official personnel record at checkout for permanent

MAR 23 2003

retention as follows: for military personnel, submit original OPNAV 5511/14 either via supporting CNO Personnel Support Detachment or directly from individual's command, as appropriate, to: Navy Personnel Command, PERS-312C, 5720 Integrity Drive, Millington, TN 38055-3120. For civilian personnel, submit original OPNAV 5511/14 either via supporting Secretariat/Headquarters Human Resource Office (S/HHRO) or directly to Human Resources Service Center Northwest, 3230 NW Randall Way, Silverdale, WA 98383.

9. Continuing Security Awareness. OPNAV (DNS-34) will periodically disseminate security posters, flyers, bulletins and newsletters to enhance security awareness of command personnel. Security coordinators and supervisors should ensure these items are displayed/routed to cognizant staff personnel for widest dissemination throughout the command. OPNAV (DNS-34) welcomes suggested security news items from all hands for including in the quarterly OPNAV Security Newsletter.

10. Waivers

a. When OPNAV security serviced activities find that fulfilling the requirements of this instruction result in an untenable sacrifice of operating efficiency, or when there are other good and sufficient reasons, a waiver of a specific requirement may be requested via OPNAV (DNS-34). Requests for waiver of DON policy requirements will be reviewed by OPNAV (DNS-34) and forwarded to CNO (N09N) for approval/disapproval if appropriate and properly justified. As guidance, the following information concerning waivers is provided:

(1) OPNAV security serviced activities currently have been granted a waiver of the requirement to maintain accountability and control records and record the destruction of routine short-life message traffic received from the Joint Communications Center. If the message traffic is received by other means, retained for file, reproduced or further disseminated, then the accountability and control requirements and destruction procedures outlined in chapters 7 and 12 apply.

(2) Accounting and control requirements for classified material can be waived.

b. Each waiver request must provide the reason why the requirement cannot be met and describes the alternative procedure that will be implemented to achieve the same result.

MAR 28 2000

Exhibit 1A

S-A-M-P-L-E

5510

Date

From: Directorate Head
To: Individual Appointed (full name, office code,
location and telephone number)
Subj: DESIGNATION AS COMMAND SECURITY COORDINATOR
Ref: (a) OPNAVINST 5510.60M
(b) SECNAV M-5510.36
(c) SECNAV M-5510.30

1. In accordance with reference (a), you are appointed as Command Security Coordinator. Your period of appointment will be for at least 1 year, from _____ until _____. You will be notified of any change in this appointment.

2. You are directed to become thoroughly familiar with references (b) and (c) as applied to your specific organization. Along with the OPNAV Security Manager (OPNAV (DNS-34)), you are to make certain that security policies are effectively implemented in a cohesive manner. You will ensure that all personnel, especially those assigned special security responsibilities, are advised of any security policy changes.

3. For effective management of the program, you shall:

a. Serve as the head advisor and direct representative of the directorate head in matters pertaining to security, and serve as the communication link between OPNAV (DNS-34) and command personnel.

b. Develop written security procedures, including an emergency plan. These procedures will be consistent with reference (a) with specifics and coverage for those items listed in chapter 1, subparagraph 3(d).

c. Coordinate and implement the security education program.

MAR 28 2000

d. Ensure that threats to security, compromise and other security violations are promptly reported, recorded and, when necessary, vigorously investigated. Monitor existing security control systems (document, physical, etc.) for effective operation.

e. Administer program for classification, declassification and downgrading of classified information.

f. Ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

g. Formulate and coordinate physical security measures for protection of classified materials.

h. Ensure security control of classified visits to include outgoing visit requests via JPAS.

i. Ensure protection of classified information during unclassified visits.

j. Ensure, where applicable, compliance with the Industrial Security Program for classified contracts with DoD contractors.

k. Ensure that all personnel who are to handle classified information or to be assigned to other sensitive duties, are appropriately cleared, and that requests for security clearances are properly prepared, submitted and monitored.

l. Ensure that access to directorate classified information is limited to those with a "need-to-know."

m. Coordinate program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

n. Ensure that appropriate security briefings and debriefings are scheduled and given to each individual departing on or returning from foreign travel.

o. Ensure that required briefings are provided to personnel before attending meetings anywhere it can be anticipated that foreign representatives will participate.

1 MAR 20 1990

p. Ensure that every required precaution is taken to prevent unauthorized disclosure when individuals are hand-carrying classified material within the command in the performance of daily duties, or outside the command in a travel status.

q. Ensure that adequate security measures are provided in advance, during, and after meetings or conferences where classified information will be disclosed.

r. Evaluate the effectiveness of the Security Program by conducting annual division security inspections per guidelines contained in exhibit 2C of reference (c) as they pertain to directorate security.

s. Assist OPNAV (DNS-34) in the identification of potential problems affecting the Security Program and report such items to OPNAV (DNS-34).

t. Assist OPNAV (DNS-34) with other security duties as required.

u. Perform those duties assigned to assistant security coordinators in their absence.

4. You are the Command Security Coordinator. Your signature below acknowledges your responsibility for this program. Your support and professionalism are necessary for success, and while each person, military, civilian and contractor, are individually responsible for our national security through compliance with security regulations, your leadership in this program ensures that security.

Designee's Signature: _____

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (OPNAV (DNS-34))

MAR 23 2000

EXHIBIT 1B

S-A-M-P-L-E

5510
date

From: Directorate Head
To: Individual Appointed (full name, office code,
Location and telephone Number)

Subj: DESIGNATION AS COMMAND ASSISTANT SECURITY COORDINATOR

Ref: (a) OPNAVINST 5510.60M
(b) SECNAV M-5510.36
(c) SECNAV M-5510.30

1. In accordance with reference (a), you are appointed as the office code Assistant Security Coordinator for _____. Your period of appointment will be for at least 1 year, from _____ until _____. You will be notified of any change in this appointment.

2. For effective management of the program, you shall:

(a) Serve as a communication link between the Security Coordinator and cognizance staff personnel.

(b) Report security violations to the Security Coordinator.

(c) Ensure that personnel under your cognizance conform to the guidance of references (a), (b), and (c) and report discrepancies to the Security Coordinator and the immediate supervisor.

(d) Relay problems or items requiring clarification to Security Coordinator.

(e) Assist the Security Coordinator with other security duties as required.

3. I request your support and professionalism in helping to carry out this vital program. At the forefront of the thoughts of all directorate personnel should be that each person,

MAR 23 2000

military or civilian, in this command is individually responsible for our national security through compliance with security regulations.

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (DNS-34)

MAR 28 2000

EXHIBIT 1C

S-A-M-P-L-E

5510
Date

From: Directorate Head
To: Individual Appointed (full name, office code,
location and telephone number)

Subj: DESIGNATION AS TOP SECRET CONTROL OFFICER

Ref: (a) OPNAVINST 5510.60M
(b) SECNAV M-5510.36

1. In accordance with reference (a), you are appointed as Directorate Top Secret Control Officer. Your period of appointment will be for at least 1 year, from _____ until _____. You will be notified of any change in this appointment.

2. You are directed to become thoroughly familiar with references (a) and (b) as they apply to your specific organization. Along with the Directorate Security Coordinator and the OPNAV Security Manager (OPNAV (DNS-34)), you are to make certain that security policies applicable to top secret material are effectively implemented in a cohesive manner. You will ensure that all personnel with top secret access, especially those assigned top secret control responsibilities, are advised of any security policy changes.

3. For effective management of the program, you shall:

a. Serve as the head advisor and direct representative of the directorate head in matters pertaining to top secret control, and serve as the communication link between the OPNAV Security Manager (OPNAV (DNS-34)) and command personnel.

b. Develop written top secret control procedures to be included in the command's security procedures. These procedures should be consistent with references (b) and (c).

MAR 28 2000

- c. Administer program for classification, declassification and downgrading of top secret information.
- d. Ensure compliance with accounting and control requirements for top secret material, including receipt, distribution, inventory, reproduction and disposition.
- e. Ensure that all personnel who are to handle top secret information are appropriately cleared.
- f. Conduct the annual inventory required by reference (a).
- g. Ensure that access to top secret information is limited to those with a "need-to-know" and records of disclosure are properly executed.
- h. Evaluate the effectiveness of the Top Secret Control Program by conducting annual division security inspections per exhibit 2C of reference (b).
- i. Perform those duties assigned to Assistant Top Secret Control Officers in their absence.

4. You are the Command Top Secret Control Officer. Your signature below acknowledges your responsibility for this program. Your support and professionalism are necessary for success, and while each person, military, civilian and contractor, are individually responsible for our national security through compliance with security regulations, your leadership in this program ensures that security.

Designee's signature: _____

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (DNS-34)

MAR 23 2009

CHAPTER 2
PERSONNEL SECURITY1. Basic Policy

a. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of his/her loyalty, reliability and trustworthiness, and the individual has executed an SF 312. The initial determination will be based on a PSI appropriate to the access level required or to other considerations of the sensitivity of the duties assigned.

b. Applicants who possess a foreign passport will be directed to surrender the passport for security clearance eligibility. The individual will destroy the passport in the presence of OPNAV (DNS-34) for documentation purposes. In addition, dual citizens will provide a signed statement expressing their willingness to renounce dual citizenship.

c. There is a U.S. citizenship requirement for personnel occupying DON sensitive and IT positions. IT access categories are based on the level of Information System (IS)/network access required to execute responsibilities of the position and the associated potential for adverse impact on the DoD mission. DoD components are responsible for designation of each position as requiring privileged, limited privilege, or non-privileged access. The sensitive IT positions are as follows:

(1) Critical Sensitive is IT-I. At this level, member has privileged access to networks and ISs, system security and network defense systems, or to system resources. Duties are broad in scope and authority and provide access to the U.S. Government, DoD, or component mission critical systems. The potential exists for exceptionally serious adverse impact on U.S. Government, DoD, component or private sector information and/or operations, with worldwide or Government-wide effects. Member may be responsible for unsupervised funds disbursements or transfers or financial transactions from IT systems of dollar amounts totaling over \$10,000 per year. U.S. citizenship is required for this level and request for waiver must have OPNAV (N09N2) approval per exhibit 5-B of reference (c).

(2) Non-critical Sensitive is IT-II. At this level, member has limited privileged access, but duties are of considerable importance to the DoD or DoD component mission, and the member is under the technical supervision of an individual

MAR 23 2003

in a higher trust position (IT-I). For example, individuals in these positions may have ability to impact a limited set of explicitly defined privileged functions, such as privileged access confined to large portions of an IS or to a local network physically isolated from other DoD or publicly accessible networks. The potential exists for moderate to serious adverse impact on DoD or component information or operations. Member may be responsible for monitored and audited funds disbursements or transfers or financial transactions from IT systems of dollar amounts totaling less than \$10,000 per year. U.S. citizenship is required for this level and request for waiver must have OPNAV (N09N2) approval per exhibit 5-B of reference (c).

(3) Non-sensitive is IT-III. At this level, member has non-privileged access to one or more DoD ISs/applications. Members at this level can receive, enter and/or modify information in an IS/application or database to which they are authorized access. Users have access only to that data/information and those applications/networks to which the member is explicitly authorized or has "need-to-know" and cannot alter those or other users' authorizations. Positive security measures and configuration management ensure that the member can assume only explicitly authorized roles and privileges. The potential exist for limited adverse impact on DoD, component or unit information or operations. Member may be responsible for financial operations subject to routine supervision or approval, but has no funds disbursement or transfer capabilities. U.S. citizenship is not required for this level.

d. In 2001, there was an amendment to Title 10, United States Code (U.S.C.), to preclude the initial granting or renewal of a security clearance by the DoD under four circumstances outlined below. Commonly referred to as the "Smith Amendment," this mandate applies to DoD civilians, contractors and military members nominated for initial security clearance eligibility, or after periodic reinvestigation for continued eligibility, who fall under one or more of the following four provisions:

(1) Conviction in any U.S. court (Federal or state court, including courts martial) of a crime, sentenced to incarceration, and, consequently, served imprisonment for a term exceeding 1 year;

(2) Unlawful user of, or is addicted to, a controlled substance (as defined in Section 102 of the Controlled Substances Act (section 802 of title 21, U.S.C.);

MAR 28 2003

(3) Mentally incompetent, as determined by a mental health professional approved by the DoD;

(4) Discharged or dismissed from the Armed Forces under dishonorable conditions.

e. Department of the Navy Central Adjudication Facility (DONCAF) will determine whether the provisions of this amendment apply to Navy or Marine Corps military or civilian members after full investigation and adjudication. The provisions of this amendment apply, regardless of whether the issues were previously considered and favorably resolved. SECNAV may authorize a meritorious waiver of the prohibitions. The determination to nominate an individual for meritorious waiver will be made by the individual's command and submitted to the DON Personnel Security Appeals Board as set forth in exhibit 8C of reference (c).

f. The OPNAV Security Manager (OPNAV (DNS-34)) is the only official authorized to request PSIs on personnel assigned to OPNAV security serviced activities for security programs. The only exception to this policy is the CNO (SSO) which has complete responsibility for PSIs on individuals who require SCI access.

g. Personnel requiring a PSI will use Electronic Questionnaire Investigations Processing (E-qip) to submit the investigation. E-qip is accessible from a secure Web site at www.opm.gov/e-qip. To gain access to the Web site, notification must be provided to OPNAV (DNS-34B) or, for personnel in SCI billets, CNO SSO. The member requiring the PSI will be sent notification when access to the Web site has been granted. Once notified by OPNAV (DNS-34B) or CNO SSO, member will have 30 calendar days to access the OPM Web site to begin the PSI or access will be terminated. Reinstatement of access will be granted either by OPNAV (DNS-34) or CNO SSO, as required, following either a phone call or e-mail notification. Before accessing the Web site to begin, member should print out the Applicant's E-qip Handbook located at www.navysecurity.navy.mil under E-qip latest updates.

h. PSI requirements are contained in chapter 6 of reference (c). Only the minimum investigation to satisfy a requirement may be requested.

MAR 28 2000

2. Request for Clearance and Access

a. All civilian and military personnel reporting aboard OPNAV security serviced activities are required to check-in with OPNAV (DNS-34), Pentagon room 5B542. During the check-in process, each individual is issued an OPNAV 5510/418 to be completed by the individual's security coordinator or assistant.

b. Security coordinators will complete the form requesting the required level of access needed for the billet, having the individual read and sign the "Security Awareness Briefing Objectives" statement on back of form and return to OPNAV (DNS-34).

c. OPNAV (DNS-34B) will initiate a request for clearance eligibility via JPAS provided the individual has an in-scope investigation required for the clearance access requested. If the individual's investigation is out of scope, OPNAV (DNS-34B) will contact the individual to arrange for either an initial investigation or periodic reinvestigation, as applicable via E-gip.

d. Until the security coordinator has received notification from OPNAV (DNS-34B) that an individual's clearance/access has been granted, access to classified information on classified local area network account (SIPRNET) is not authorized. Access without this notification constitutes a security violation.

e. When a final clearance eligibility has been granted by DONCAF, the information will post in JPAS, and OPNAV (DNS-34B) will take the following action:

(1) Individual's JPAS record will be updated to reflect final clearance eligibility and "United States" access will be granted.

(2) Update individual's record in OASIS for the cognizant office assigned.

f. An urgent operational emergency may arise for cleared personnel to have one-time or short duration access to classified information at a level higher than that for which they are eligible. Processing the individual to upgrade the security clearance would not be practical in these situations, therefore, an individual may be granted access at one security classification level above that for which he/she is eligible, subject to the following terms and conditions:

MAR 23 2003

(1) A flag officer or general officer, a general courts-martial convening authority, or equivalent SES member, may grant one-time access, after coordination/concurrence with OPNAV (DNS-34).

(2) The individual granted one-time access must be a U.S. citizen, have a DoD security clearance eligibility determination and have been continuously employed by DoD or a cleared DoD contractor for the preceding 24-month period. One-time access is not authorized for part-time or temporary employees.

(3) A review of locally available records must reveal no disqualifying information.

(4) Whenever possible, access will be limited to a single instance or, at most, a few occasions. If repeated access is required, the proper PSI will be initiated.

(5) The access authorization will automatically expire no later than 60 calendar days from the date access commenced. If the need for access is expected to continue for a period in excess of 60 days, the command must initiate a request for the appropriate PSI. Access will not be extended, in any case, beyond 60 days from the date access commenced unless a supporting PSI is requested.

(6) Access at the higher level will only be allowed under the supervision of a properly cleared individual.

(7) Access will be limited to information under the control of the official who authorized the one-time access. One-time access will not be authorized for Communications Security (COMSEC), SCI, NATO or Foreign Government Information (FGI).

g. One-time access will be used sparingly, and repeated use of one-time access within any 12-month period on behalf of the same individual is prohibited.

h. A record must be maintained for each individual authorized one-time access. A letter will be generated to OPNAV (DNS-34) with the following information:

MAR 23 2003

(1) Justification for the access will be recorded, to include an explanation of the compelling reason for granting the higher level access and, specifically, how the DON mission is being furthered;

(2) An unclassified description of the specific information to which access was afforded and the duration of the access, to include the dates access was afforded;

(3) A description of the specific results of the local records review; and

(4) The approving authority will be fully identified with name, rank and position.

3. Emergency Appointment to Sensitive Positions for Civilians

a. When an appointee does not have the necessary investigative basis for appointment, he/she may be placed in a non-critical sensitive position only as an emergency measure after the directorate head determines that delay in appointment would be harmful to national security, the Access National Agency Check with Written Inquiries (ANACI) has been requested, and a check of locally available records is favorable. The directorate head's justification for the emergency appointment will be recorded in writing. The record of emergency appointment letter will include the following:

(1) Identifying data on the appointee to include full name, social security number, date and place of birth, position or job title;

(2) Organizational location of the position;

(3) Position sensitivity and designation criterion;

(4) Certification and justification by the directorate head that emergency appointment is necessary. (In determining whether emergency appointment is justified, a delay in appointment may be considered harmful to the national security if regulatory requirements and mission-essential functions or responsibilities cannot be met and no other cleared or otherwise qualified personnel are available on a temporary basis to do the work);

(5) A statement that a check of locally available records was favorable; and

MAR 28 2000

(6) The date that the required PSI was requested. For a critical-sensitive position, the record will also include the date of the National Agency Check with Local Agency and Credit Checks (NACLCC) or ANACI that formed the basis for emergency appointment.

b. To keep emergency appointments to the absolute minimum, the need to fill a sensitive position must be anticipated and a request for the required investigation sufficiently requested in advance of the desired date of appointment.

c. OPNAV security serviced activities must submit an emergency appointment letter including a request for interim access (see example in exhibit 2A) to OPNAV (DNS-34) with information copies to S/HHRO and the cognizant security coordinator.

d. A pre-appointment background investigation is required for a critical sensitive position. In an emergency, a critical sensitive position may be occupied pending completion of an SSBI by OPM when a NACLCC or ANACI has been favorably completed. An emergency appointment letter, including a request for interim clearance (see example in exhibit 2B) must be submitted to OPNAV (DNS-34) with information copies to S/HHRO and the cognizant security coordinator. There is no provision for appointment to a critical sensitive position when the individual does not have any valid investigative basis.

e. In case of an individual who has submitted an investigation for a critical sensitive position but has no prior investigation basis for an interim, once OPM has completed the National Agency Check (NAC) portion, interim access can be granted.

4. Classified Information Nondisclosure Agreements

a. An SF 312 is to be executed by all cleared Government and non-government personnel as a condition of access to classified information.

b. All personnel (military or civilian) are required to execute an SF 312 as part of their check-in procedure with OPNAV (DNS-34), unless verification can be made that a valid SF 312 has previously been executed and remains valid for the individual via JPAS.

MAR 28 2008

c. Refusal to execute the SF 312 will be grounds for denial of access to classified information.

5. Continuous Evaluation of Eligibility

a. Personnel security responsibilities do not stop once a favorable determination is made. Any person having knowledge or information reflecting on an individual's loyalty, reliability and trustworthiness from a security perspective will immediately report the full particulars and circumstances to OPNAV (DNS-34) for evaluation and/or further investigation.

b. Self reporting requirements were implemented by Under Secretary of the Defense memo dated 2 April 2008; all commissioned officers, warrant officers, and enlisted members over the pay grade E-6 who are on active duty or in an active status in a Reserve Component shall report, in writing, any conviction of such member for a violation of a criminal law of the United States whether or not the member is on active duty or in an active status at the time of the conduct that provides the basis for the conviction. Active duty members must report under this policy within 15 days of the date the conviction is announced, and reservists not on active duty but in an active status shall report at first drill period after date of conviction announced, regardless of whether sentence has been imposed or member intends to appeal conviction.

c. S/HHRO, security coordinators/ASCs, command legal staff, Government Credit Card Program coordinator and, in particular, supervisors are cautioned that information which could place an individual's loyalty, reliability and trustworthiness in question has to be evaluated from a security perspective. All are hereby required to familiarize themselves with the adjudication policy contained in exhibit 10A of reference (c). Behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct is potentially significant to an individual's security status and information concerning these issues must be immediately reported to OPNAV (DNS-34).

d. Co-workers have an equal obligation to advise their supervisor, security coordinator or OPNAV (DNS-34) when they become aware of information with potentially serious security significance regarding an OPNAV member with access to classified information or employed in a sensitive position.

MAR 28 2003

6. Administrative Withdrawal of Adjustment of Clearance

a. The security clearance of an individual will be administratively withdrawn, without prejudice, when there is no need for access to classified information in connection with his/her official duties. Clearance will be administratively adjusted when the level of access required for official duty changes, provided the appropriate investigative basis for the required clearance exists.

b. When a clearance is administratively withdrawn, the individual will be debriefed by the cognizant security coordinator/ASC in accordance with paragraph 4-11 of reference (c). The executed OPNAV 5511/14 will be forwarded to OPNAV (DNS-34) for mailing and filing in the official personnel record.

c. Administrative withdrawals or lowering of security clearance access is not authorized for cause (i.e., when disqualifying information about the individual is known). A resulting unfavorable personnel security determination by DONCAF may result in denial or revocation of clearance.

d. When security clearance access is administratively withdrawn or lowered, OPNAV (DNS-34B) will update JPAS to show that the action was taken administratively and without prejudice to the individual.

e. Security clearance eligibility which was administratively withdrawn or lowered may be reinstated to the previous level if access requirements for official duties change. After favorable review of locally available records, clearance level may be re-adjusted.

7. Denial or Revocation of Clearance/Access for Cause

a. When a personnel security determination has been made that an individual does not meet or no longer meets the criteria for security clearance eligibility, the clearance will be denied or revoked for cause by DONCAF.

b. Denial or revocation of security clearance for cause is an unfavorable personnel security determination, as described in chapter 8 of reference (c). On revocations, the individual will be debriefed in accordance with paragraph 8 of this chapter, and

[REDACTED]

the OPNAV 5511/14 will be completed and forwarded to OPNAV (DNS-34) for mailing and filing in the individual's official personnel record.

c. When a DON civilian is incarcerated as the result of conviction for a criminal offense, or is absent without leave for a period exceeding 30 days, or when a military member is adjudged punitive discharge or incarcerated as the result of conviction for a criminal offense, or is declared a deserter, OPNAV (DNS-34) will revoke security access immediately and without regard to unfavorable action procedures. The report of revocation will be forwarded by OPNAV (DNS-34B) to DONCAF.

d. Request for security clearance and/or assignment to a sensitive position, following a final unfavorable personnel security determination, may be resubmitted after 12 months from the original decision. A determination must be made that the individual meets the criteria for a clearance and a need for the clearance must also exist. Request for eligibility determination must be made to DONCAF.

e. When a request is received to consider eligibility, following an unfavorable personnel security determination, OPNAV (DNS-34B) will not grant interim security clearance nor will the requesting office assign the individual to sensitive duties until a final decision is made by DONCAF.

8. Suspension of Access

a. When questionable or unfavorable information becomes available concerning an individual, OPNAV (DNS-34), in coordination with assigned command authorities, may decide to limit or suspend access. Limitation or suspension of access for cause may only be used as a temporary measure until the individual's eligibility for access has been resolved.

b. When effecting limitation or suspension of access, OPNAV (DNS-34) will:

(1) Advise the individual, in writing, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security;

(2) Report suspension to DONCAF via JPAS within 10 working days, detailing the questionable or unfavorable action for suspension;

MAR 23 2339

(3) Take steps to ensure that the individual's name is removed from all local access rosters, records and visit certifications, as well as SIPRNET cancelled or limitation noted, and that all coworkers are notified;

(4) Ensure that the combination to classified storage containers, to which the individual had access, are changed; and

(5) Post a notice of limitation or suspension of access in the individual's personnel file, pending final resolution on the individual's eligibility by DONCAF.

c. Individuals that are allowed to work in a open classified storage space without the proper access must be escorted at all times.

9. Clearances Under DoD Industrial Security Program.

Instructions for clearance under the DoD Industrial Security Program are contained in chapter 15 of this instruction.

10. Access to CNWDI

a. Because of the extreme sensitivity of CNWDI, access to and dissemination of CNWDI information must be limited to the minimum number of persons who require it in the performance of their official duties. To meet this objective and ensure that security policy guidance is strictly observed, special administrative controls have been established at exhibits 2C through 2F to outline procedures and positively identify those personnel requiring access to CNWDI.

b. OPNAV security serviced activities outlined at exhibit 2G will implement the procedures outlined in exhibits 2C through 2F for those personnel under their cognizance requiring access to CNWDI.

c. OPNAV security serviced activities or their designated representatives are responsible for maintaining personnel clearance and security briefing forms and notifying OPNAV (DNS-34) of deletions to the listing of authorized personnel (exhibit 2E) as they occur; exhibit 2D will be completed to document debriefing of personnel.

11. Debriefings. The requirements and criteria for debriefing personnel who had access to classified information are contained in paragraph 8 of this chapter.

MAR 23 2003

EXHIBIT 2A

S-A-M-P-L-E

5520
Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (OPNAV (DNS-34))

Subj: EMERGENCY APPOINTMENT TO A NONCRITICAL SENSITIVE
POSITION

Ref: (a) OPNAVINST 5510.60M
(b) SECNAV M-5510.30

Encl: (1) Security Indoctrination Certification and
Request for Clearance

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated non-critical sensitive:

Full Name: DOB: POB:
SSN: Position/Job Title:

2. A National Agency Check and Inquiry/National Agency Check on (Name)_____, (Grade), was submitted to the Office of Personnel Management/Defense Investigative Service on ___(Date)___ and local records check was favorable. A request for security access is submitted as enclosure (1). Request an interim secret clearance be granted per reference (b).

3. This exception is necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. _____(Name)_____, (OPNAV NCode/Navy Staff Office) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

5. It is understood that interim secret clearance is automatically cancelled 6 months from the date granted, upon granting final access, or upon transfer to duty outside (your division).

OPNAVINST 5510.60M

MAR 23 2009

Copy to:
Cognizant Security Coordinator
S/HHRO

MAR 23 2003

EXHIBIT 2B

S-A-M-P-L-E

5520

Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (OPNAV (DNS-34))

Subj: EMERGENCY APPOINTMENT TO A CRITICAL SENSITIVE
POSITION

Ref: (a) SECNAV M-5510.36
(b) OPNAVINST 5510.60M

Encl: (1) Security Indoctrination Certification and
Request for Clearance

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated critical sensitive:

Full Name:	DOB:	POB:
SSN:	Position/Job Title:	

2. A Background Investigation/Special Background Investigation on _____ (Name), (Grade), was requested on _____ (Date). A satisfactory NAACL/ANACI was completed on _____ (Date) by the Office of Personnel Management/Civil Service Commission/Defense Investigative Service. A request for security access is submitted as enclosure (1). It is requested that an interim top secret clearance be granted per reference (b).

3. This exception is necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. _____ (Name), _____ (OPNAV NCode/Navy Staff Office) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

MAR 23 2009

5. It is understood that interim top secret clearance is automatically cancelled 6 months from the date granted, upon granting final access, or upon transfer to duty outside (your division).

Copy to:
Cognizant Security Coordinator
S/HHRO

MAR 23 2009

EXHIBIT 2C

S-A-M-P-L-E

PROCEDURES FOR CERTIFYING ACCESS TO CRITICAL NUCLEAR WEAPONS
DESIGN INFORMATION (CNWDI)

1. Screening Procedures. Prior to certifying an individual for access to CNWDI, the following prerequisites must be verified:

a. The prospective recipient must have a valid DoD security clearance (final top secret or secret) based on the appropriate investigative requirements.

b. The prospective recipient must require access to nuclear weapons design information in the performance of his/her official duties. Strict adherence to the "need-to-know" principle must be observed.

2. Certification Procedures. The following procedures are to be followed when certifying an individual for access to CNWDI:

a. Verify the basic prerequisites outlined in paragraph 1 above.

b. Execute the interoffice memo outlined in exhibit 2E, ensuring that the appropriate certifying officials (at exhibit 2G) sign the document. Document may also be signed as "for," "by direction," or "acting," as appropriate, in the absence of the certifying official.

3. Update Procedures

a. Additions. Conduct screening, certification and submit interoffice memo in accordance with paragraphs 1 and 2 above.

b. Deletions. Provide copy of signed Debriefing Certificate to OPNAV (DNS-34).

MAR 23 2003

EXHIBIT 2D

S-A-M-P-L-E

BRIEFING/DEBRIEFING CERTIFICATE

CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION

PART I

1. I acknowledge that I have been authorized to receive or hold Critical Nuclear Weapons Design Information. I understand that the security of Critical Nuclear Weapons Design Information is of paramount importance and that unauthorized disclosure of such information will endanger the United States.

2. I understand that when I have a change in my assignment or duty which makes it no longer necessary for me to have access to Critical Nuclear Weapons Design Information, I must execute a Debriefing Certificate.

3. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, if I discuss with, or disclose Critical Nuclear Weapons Design Information to any person not currently authorized to have such information.

(Date)
(Signature of Witness)

(Signature)
(Name Printed or Typed)

PART II

1. I acknowledge that I am no longer authorized access to Critical Nuclear Weapons Design Information. I certify that, hereafter, I will not divulge or discuss such information which I have acquired as an authorized recipient, unless required to do so by a competent authority.

2. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, for any unauthorized disclosure.

(Date)
(Signature of Witness)

(Signature)
(Name Printed or Typed)

MAR 23 2000

EXHIBIT 2E

S-A-M-P-L-E

5210

Date

From: (OPNAV Security Serviced Activities)
To: OPNAV Security (DNS-34)

Subj: CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION,
CERTIFICATION OF NEED-TO-KNOW

Ref: (a) DoD Directive 5210.2
(b) OPNAVINST 5510.60M

Encl: (1) Personnel certified for access to Critical
Nuclear Weapons Design Information

1. Per references (a) and (b), the personnel listed in enclosure (1) are certified as having a "need-to-know" for Critical Nuclear Weapons Design Information (CNWDI).
2. Briefing certificate(s) has/have been completed.

(Signed by Certifying Official)

MAR 23 2009

EXHIBIT 2G

S-A-M-P-L-E

List OF OPNAV Security Serviced Activities CNWDI Certifying
Official

Secretary of the Navy
Under Secretary of the Navy
Assistant Secretary of the Navy (Research, Development &
Acquisition)
Assistant Secretary of the Navy (Manpower & Reserve Affairs)
Administrative Aide to the Secretary of the Navy
Director, Office of Program Appraisal
Chief of Naval Operations (N00)
Vice Chief of Naval Operations (N09)
Director Navy Staff (DNS)
Director of Naval Intelligence (N2)
Director of Navy Test & Evaluation & Technology Requirements
(N091)
Director, Test & Evaluation Division (N0912)
Deputy Chief of Naval Operations (Manpower, Personnel, Training
& Education) (N1)
Deputy Chief of Naval Operations (Plans, Policy & Operations)
(N3N5)
Deputy Chief of Naval Operations (Fleet Readiness & Logistics)
(N4)
Director, Supply, Ordnance, & Logistics Operations Division
(N41)
Deputy Chief of Naval Operations (Integration of Capabilities &
Resources) (N8)
Surface Warfare Branch (N86)
Submarine Warfare Branch (N87)
Air Warfare Branch (N88)

MAR 23 2009

CHAPTER 3
BUILDING BADGES, PROPERTY PASSES AND
CONTROL ACCESS CARD (CAC) ISSUANCE

1. DoD Building Passes

a. Background. The Washington Headquarters Services (WHS), Physical Security Division is responsible for setting policies for issuance of DoD building passes. Day-to-day operations and management of the issuance of the DoD building passes reside with the Pentagon Building Pass Office, located in room 1F1084. OPNAV (DNS-34) is assigned authority for documenting, processing and issuing applications for DoD building passes for those individuals assigned to OPNAV security serviced activities.

b. Requirements for possession and use of DoD building passes:

(1) Badges will be issued minimally for 1 month and not to exceed 31 December 2010 when they are scheduled to be replaced by the CAC. Each individual, military or civilian, shall show his/her pass to police officers upon entering the Pentagon. Additionally, the DoD building pass must be displayed visibly on outer clothing at all times. Building pass holders must exercise proper precautions to prevent loss of their passes. In the event a pass is lost, however, the loss must be reported immediately to the Pentagon Building Pass Office. Pentagon Building Badge Office will replace the badge upon receipt of verbal loss notification without the signed DD 2249 DoD Building Pass Application.

(2) A favorably adjudicated investigation is required for issue of a permanent building pass. A temporary badge will be issued upon completion of National Criminal Investigation Check (NCIC) to new members upon arrival onboard to allow for completion of the E-qip investigation requirements. Advance coordination is required between the S/HHRO and OPNAV (DNS-34) due to the processing lead time of 3 to 5 days for NCIC.

(3) Specific type of building pass will be issued to new employees and visitors upon verification of identification as follows:

(a) DD 1466 DoD Building Pass (White Background), Government employees.

MAR 23 2009

(b) DD 1466 DoD Building Pass (Pink background), contractor personnel.

(c) DD 1466 DoD Building Pass (Blue Background), press.

(d) DD 1466 DoD Building Pass (Tan Background), foreign nationals.

(4) Request for temporary Badges will include name, Social Security Number (SSN), Date of Birth (DOB), country of birth, physical description and citizenship. Temporary badges will cover periods of 1 to 11 months only.

(5) Type of Badges: National Capital Region (NCR) (unrestricted access to DoD buildings), PNT (24-hour access to the Pentagon), PNT/NC (24-hour access to Pentagon and Crystal City) and Federal Office Building #2 (FOB#2) (24-hour access to Navy Annex). PNT badge allows unrestricted access to the Navy Annex.

(6) Access Privileges:

(a) Visitor Access Control Program. The visitor's command must send a visit notification to the Pentagon Building Pass Office at least 3 days prior to the visit. The individuals will be issued a "Visitor, No Escort Required" pass. The letter will be faxed via the Navy's point of contact in the Pentagon for security coordinator's approval. The security coordinator will then fax the request to the Pentagon Building Pass Office, (703) 697-9085, or mail it to the Pentagon Force Protection Agency (PFPA), Attn: Pass Office, Washington Headquarters Services, 1155 Defense Pentagon, Washington DC, 20301-1155. Visitors names will be added to the visitors' roster located at the Metro entrance to the Pentagon. The request must include the full name, SSN, location, DOB, PSI date (do not include clearance, i.e., secret, top secret or SCI), dates of visit, point of contact in the Pentagon and phone number, and a point of contact in the originating agency. Period of coverage may be for up to 1 year or may be submitted for individual dates. Once appropriate visit notification has been submitted, the potential visitor may enter the Metro entrance of the Pentagon and present two forms of Identification (ID). After confirmation of name on the visitors' roster, the visitor will be issued a "Visitor, no Escort Required" pass.

MAR 23 2009

(b) Escort. Privileges are not automatic, however, personnel with the white or pink background DoD pass may escort up to 3 visitors (unless the "NE" (for "no escort" privileges) designation is present on the front of the pass). Blue background pass holders have limited escort privileges. Tan, red and visitor pass holders have no escort privileges. DoD personnel with escort privileges (escort officials) must remember that it is their responsibility to stay with their visitors at all times while in the building.

(c) Armed. Any armed person, who provides personal protection for a visitor to the Pentagon, shall notify PFFA, in writing, in advance. Telephone notification is authorized for short notice visit. Denoted by "A" on the badge, armed category is given to any DoD member who is required to carry weapon in duty capacity on the Pentagon Reservation. A letter requesting approval must be submitted to PFFA via OPNAV (DNS-34). The above process will also be used to request approval for weapon displays; note that firing pins must be removed from weapons, explosive devices must be inert, and no ammunition may accompany the weapon. The following information is required: the date and time-of-entry, place of entry, name of individual carrying the weapon or explosive, room number of the office to be visited.

(d) Continuity Of Operations Plan (COOP). Identified by a "3" on a badge for members that may require free movement on the Pentagon Reservation during crises. OPNAV (DNS-34) has approval for initial COOP badges issuance only. A listing is maintained by the Pentagon Building Pass Office for replacement or renewing badges with COOP requirements.

(e) Exception to Policy. Is the venue for four and more escort requirements. One escort is required for every six visitors; 2 escorts required for every 12 visitors; 3 escorts required for every 18 visitors (1 in the front, 1 in the back, and 1 on the side of the group); 4 escorts required for every 24 visitors (1 in the front, 1 in the back, and 1 on each side); 6 escorts required for every 30 visitors (1 in the front, 1 in the back, 1 on each side of the group, and 2 trailing the group). Forward the request to the Pentagon Access and Control Office. The Pentagon Access and Control Office can also accept a fax, however, their preference is to receive requirement via e-mail. The fax number is (703) 697-9085. Call (703) 693-3953 for specific e-mail instructions.

MAR 23 2009

1. Name of event/date/time;
2. Number of persons in your party;
3. Entrances to be utilized;
4. Purpose of visit;
5. Complete name and phone number;
6. Name of escorts.

c. Issuance and Accountability Procedure. Each DoD component will appoint Authorizing Official (AO), who is responsible for the sponsoring the applicant for access to buildings on the Pentagon Reservation. The AO must be a United States citizen and a DoD Government employee. AO will not be appointed based on grade or position. DoD components will appoint those personnel whose duties coincide with the ability to be readily accessible to telephone queries from the Pentagon Building Pass Office to respond to questions or verify information on DD 2249s submitted for a building pass. The Pentagon Building Pass Office will, upon encountering problems on DD 2249s, make every effort to contact the responsible AO, thereby providing optimum customer service to the applicant. The three Navy AOs which have been designated by the DNS are located in Pentagon room 5B542 in the OPNAV Security Office.

d. Denial, Revocation or Non-renewals. Pentagon Building Pass Office will decide as a result of a routine security background check to deny the issuance of a DoD building pass. If denied, member will receive a letter via OPNAV (DNS-34) from Pentagon pass officer to respond for an interview within 30 days.

2. Procedures for Badge Issuance

a. Military and civilian employees. DD 2249s are issued from OPNAV (DNS-34), in the OPNAV Security Office, for all military and civilian personnel permanently stationed or employed by OPNAV security serviced activities.

b. Contractors

(1) Memorandum for building pass requests for DoD building passes for contractors will be considered on a case-by-case basis. Requests must be in writing, submitted to OPNAV

MAR 23 2009

(DNS-34) by the point of contact and endorsed by the security coordinator. Building pass requests must also be accompanied by the original visit request from the contracting company. Requests must also specify frequency of access required by the contractor, room number to be visited, and briefly justify the need for a building pass. Approved requests will provide passes for the length of time specified on the accompanying visit request, or as specified on the memorandum for building request pass. The point of contact is responsible for notifying contractor(s) of approval/disapproval of building pass request and for providing an escort to accompany the contractor to the OPNAV Security Office and the Pentagon Building Pass Office. DD 2249 for contractors are issued from OPNAV (DNS-34D).

(2) Requests for contractor building passes will be approved if the member provide direct support or benefit to the command and not as a matter of convenience to the contractor. Concurrently, passes will not be issued to employees of contractor facilities not within commuting distance of the Pentagon, or to employees of contractor facilities who are under contract with another government agency in the NCR. NCR passes will be issued to contractors on case by case instances as reviewed by OPNAV (DNS-34).

c. Reserve Military Personnel

(1) Military personnel from reserve units drilling within the Pentagon or swing spaces will be issued DoD building passes based on orders or a list provided from the commanding officer of their reserve unit certifying their clearance and investigation information to OPNAV (DNS-34). Passes will not exceed expiration date of 31 December 2010. DD 2249s are issued from OPNAV (DNS-34) in the OPNAV Security Office.

(2) Military personnel assigned to OPNAV security serviced activities drilling for a short timeframe (usually 30 days minimal) within the Pentagon, and swing spaces will be issued a temporary pass upon presentation of valid orders.

d. Military and civilian employees visiting from other Government commands

(1) Requests for DoD building passes to visit OPNAV offices will be considered on a case-by-case basis. Requests must be in writing, submitted, and endorsed by the security coordinator. Requests must also be accompanied by the original visit request (endorsed by OPNAV (DNS-34) as outlined in chapter

MAY 28 2000

14). Requests will specify frequency of access required by the visitor, the office to be visited, and briefly justify the need for a building pass. Approved requests will provide passes for the length of time specified on the accompanying visit request, or the memorandum request for building pass. The security coordinator is responsible for notifying visitor(s) of approval/disapproval of building pass request, and for providing an escort to accompany the visitor during building pass processing. DD 2249s for visitors are issued from OPNAV (DNS-34) in the OPNAV Security Office.

(2) Requests for visitor building passes will be approved if the member provides direct support or benefit to the command and not as a matter of convenience to the visitor. Concurrently, passes will not be issued to employees of other Government commands not within commuting distance of the Pentagon unless visit request indicates the individual is temporarily assigned to OPNAV security serviced activities nor to employees of Government commands within the NCR authorized to issue DoD building passes. Active Duty military and DoD civilian personnel may use their CAC and another form of ID to enter and exit the Pentagon during normal working hours (0600-2000). NCR passes will only be issued to visitors of those offices predetermined by OPNAV (DNS-34) to justify such passes when requested by the security coordinator.

e. All personnel reporting for a DoD building pass must present a photographic I.D. (such as valid driver's license, other Government ID card, expiring DoD building pass, or military ID card) and a second Government form with verification of SSN. Personnel escorting prospective pass recipients must remain with and are responsible for the prospective pass recipients until completion of pass issuance at the Building Pass Office.

3. Property Passes

a. The removal of property from the Pentagon and other DoD locations is governed by WHS, Physical Security Division, and PFPA. Regulations require that the authorized removal of Government property not covered by a bill of lading or invoice shall be accomplished by OF 7 Property Pass, or memorandum on official business letterhead including description of the property and date of issue. The property pass or memorandum will be given to PFPA officers when exiting the building.

MAR 23 2003

b. Accountability for Government property within OPNAV is under the cognizance of the director, OPNAV security serviced activities. OPNAV security serviced activities report to DNS for accountability of Government property under their control. Within SECNAV activities, accountability for Government property is under the cognizance of the Director, Facilities Services and Support Division/AAUSN.

4. Contractor Verification System (CVS). Sponsored by the Defense Manpower Data Center (DMDC), as directed by Homeland Security Presidential Directive-12, is an automated process to authorize the issue of a CAC to DoD contractors.

a. CVS is a Web-based application that receives automatic personnel data from the Defense Enrollment and Eligibility Reporting System (DEERS), eliminating paperwork for issuance of CAC to contractors. Electronic applications are processed, reviewed and stored by delegated Trusted Agents (TAs) at the command level. OPNAV security serviced activities are responsible for appointment of TAs; or a TA can be concurrently staffed by the command's security coordinator. OPNAV Security Branch personnel (OPNAV (DNS-34/34B/34D)) will serve as the TA security manager under the CVS. TAs will initiate contractor's CAC request in the system. Contractors must have submitted information required for the issuance of a CAC using the CVS Web application. Specifically, the contractor logs into CVS using the temporary user ID and password automatically generated by the system and distributed to the contractor by the TA. The contractor will be able to save a partially completed application; however, the application will not be processed until it has been submitted in complete format. Once completed and application is submitted, the system automatically notifies the TA. The TA then logs into CVS using his/her CAC or his/her username/password and reviews and approves or rejects the application. If rejected, the system notifies the contractor and electronically records the rejection. CVS will automatically update DEERS with the contractor's information and direct the contractor via e-mail to proceed to a Real-Time Automatic Personnel Identification System (RAPIDS) workstation for CAC issuance.

b. CACs are revalidated every 6 months by TAs upon automatic system notifications which are initiated by the DMDC.

MAR 23 2009

CHAPTER 4
CLASSIFICATION1. Basic Policy

a. Reference (a) is the basis for classifying national security information except as provided in the Atomic Energy Act of 1954, as amended. It is DON policy to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information will be classified only to protect national security.

b. Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, safeguard it as if it were classified at appropriate level pending a determination by an OCA. When there is reasonable doubt about the appropriate level of classification, safeguard the information as if it were classified at the higher level until an OCA makes a determination. The OCA's determination must be made within 30 days (see paragraph 4-12 of reference (b)).

2. Classification Designations

a. Information which requires protection against unauthorized disclosure in the interest of national security must be classified with one of only three designations:

(1) Top Secret. This designation is applied only to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security. Examples include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting national security; the compromise of vital national defense plans or complex crypto logic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) Secret. This designation is applied only to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security. Examples include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or

MAR 23 2009

intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) Confidential. This designation is applied only to information, the unauthorized disclosure of which could reasonably be expected to cause damage to national security. Examples include information indicating strength of ground, air, and naval forces; performance characteristics, test data, design, and production data on U.S. weapon systems and munitions.

b. The markings "For Official Use Only" and "Limited Official Use" cannot be used to identify classified information, nor can modifying terms be used in conjunction with authorized classification designations, such as "Secret Sensitive".

3. For Official Use Only (FOUO)

a. FOUO applies to information, records, and other materials which have not been given a security classification under the criteria of an Executive order, but which contain information which may be withheld from the public for one or more of the reasons cited in Freedom of Information Act (FOIA) exemptions 2 through 9 per reference (h). No other material shall be considered or marked FOUO, as FOUO is not authorized as a form of classification to protect national security interests.

b. Unclassified documents and materials containing FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one). Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom. Each paragraph containing FOUO information will be marked with the abbreviation FOUO in parentheses at the beginning of the FOUO portion. Material other than paper documents (slides, computer media, films, etc.) will bear markings which alert the viewer that the material contains FOUO information. FOUO documents and material transmitted outside DoD must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information as follows:

"This document contains information
exempted from mandatory disclosure under FOIA.
Exemption(s) -- apply."

MAR 23 2009

c. When information is contained within a classified document, full pages containing FOUO information, but no classified information, shall be marked "FOR OFFICIAL USE ONLY" at both the top and bottom of the page. Portions on that page require specific FOUO marking as an indication to holders that the information requires additional control.

d. Safeguard, dissemination and transmission: FOUO information will be handled in accordance with security procedures. FOUO is used as a means to alert the reader that the document may contain material that is exempted from disclosure. During working hours, steps will be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO may be stored as a minimum in unlocked containers, desks or cabinets if Government or Government-contracted building security is provided. If Government or Government-contract building security is not provided, it must be stored at a minimum in a locked desk, file cabinet, bookcase, locked room, or similar place. FOUO documents and material may be transmitted via first class mail, parcel post, or fourth class mail for bulk shipments. Fax or e-mail transmissions of FOUO information (voice, data, or facsimile) will be by encrypted communications systems when ever practical. FOUO information may be put on an Internet Web site only if access to the site is limited to a specific target audience and the information is encrypted. FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in a regular burn bag. This requirement is due primarily to the personal nature of FOUO being worked.

4. Original Classification Authority

a. The authority to originally classify information as top secret, secret or confidential has been granted by SECNAV to officials listed in chapter 4, exhibit 4A of reference (b). Authority to originally classify at a level lower than the one listed is inherent in the designation.

b. Original confidential classification authorities are not specifically designated. Original confidential classification determinations will be made by original top secret and secret classification authorities.

c. Only the incumbents of the positions listed in chapter 4, exhibit 4A of reference (b) have OCA, and this authority is

[MAR 28 2000]

non-delegable. If an OCA is absent, however, the person designated to act in his/her absence may exercise the classification authority.

d. OPNAV (DNS-34) maintains a current list of OPNAV/SECNAV/DON staff office officials designated as original top secret and secret classification authorities, and ensure that they are trained in their classification responsibilities. OPNAV (N09N2) conducts an annual review of continuing need for OPNAV officials to exercise OCA authority. OCAs will maintain an accurate list of classification decisions for annually reporting via OPNAV (N09N2) to Information Security Oversight Office (SF-311, Agency Security Classification Management Program Data, applies per reference (b), appendix C).

e. Submit requests for OCA to OPNAV (N09N2) via OPNAV (DNS-34). Each request must identify the nominee's position, title and organization and describe the circumstances in each of the areas contained in paragraph 4-5 of reference (b) that justify the delegation of such authority.

f. All original classification authorities must be indoctrinated in the fundamentals of security classification, limitations of their authority to classify and their responsibilities. The indoctrination is a prerequisite to granting OCA and shall be a matter of record subject to audit. OPNAV (N09N2) has developed a program to ensure indoctrination of all current authorities and this program is implemented for all OCAs under CNO's cognizance. OPNAV (DNS-34) will initiate the required action with personnel reporting aboard into a billet previously authorized as an OCA. The authority does not automatically carry forward with the newly reporting official until completion of the required indoctrination procedures.

5. Original and Derivative Classification

a. Original classification is the initial two-part determination that information requires, in the interest of national security, protection against unauthorized disclosure and a determination of the level of protection required. For example, a missile program manager determines that certain operational characteristics, such as speed, range and lethality, require classification at the confidential level to ensure the missiles operational superiority throughout its life cycle. Those original classification determinations are issued as part of the program SCG. Subsequently, any time that information is used, by anyone in any form, it is derivatively classified

11/20/11

confidential based on that original classification determination. Duration of initial classification will not exceed 25 years from date of original classification. When the information has been initially given a duration date of less than 25 years, and the cognizance OCA latter extends protection up to 25 years, holders of the classified information will be notified.

b. Derivative classification can be accomplished by anyone who incorporates, paraphrases, restates, or generates, in new form, information which is already classified. Derivative classification is most commonly accomplished by marking material per guidance from an OCA. An estimated 99 percent of the classified information produced by DON commands is derivatively classified (i.e., based on a classified source document or an SCG (5513 series)). If it is believed that paraphrasing, restating, or summarizing of classified information has changed the level of, or removed the basis for, classification, the cognizance OCA will be asked for a specific determination which is to be made within 30 days of receipt of the request.

c. A derivative classifier must comply with the requirements contained in paragraphs 4-9 of reference (b) and reference (i).

d. Refer to chapter 4 of reference (b) for other detailed measures regarding classification of information.

6. Security Classification Guide

a. SGCs are recordings of DON original classification determinations for security management and program use. SCGs serve as the primary reference source for derivative classifiers to identify the level and duration of classification for the specific information elements.

b. DON OCAs are required to prepare an SCG for each DON system, plan, program, or project under their cognizance which creates classified information. SCGs shall be issued as soon as practicable prior to initial funding or implementation of the relevant system, plan, program, or project. SGCs shall be prepared in writing, in the format described in reference (j), and approved personally by an OCA who has both cognizance (i.e., program or supervisory responsibility) over the information, and who is authorized to originally classify information at the highest classification level prescribed in their SCG(s).

MAR 23 2009

c. After approval by an OCA, SCGs are forwarded to OPNAV (N09N2), Retrieval and Analysis of Navy Classified Information (RANKIN) program manager, and entered into the RANKIN data base. Additionally, the RANKIN program manager at OPNAV (N09N2) maintains historical files for all DON SCGs.

d. OCAs shall review their SCGs for accuracy and completeness at least every 5 years and advise OPNAV (N09N2) of the results. Proposed changes to, and cancellations of, existing SCGs shall be sent to OPNAV (N09N2) in the format described in reference (j).

7. Industrial Operations

a. Industrial management does not make original classification determinations but applies the classification decisions of the Government contracting authority. Classification in industrial operations under DON contracting authority will be based strictly on security classification guidance furnished by DON. Reference (k) requires contractors to apply the classification guidance accurately and uniformly to their operations.

b. OPNAV security serviced activities are required by references (b) and (c) and chapter 15 of this instruction to use DD 254 to convey specific contractual security classification guidance to their contractors. The appropriate SCGs (promulgated by the 5513 series of OPNAV instructions) or other written narrative SCG will be provided via the DD 254, as appropriate. Each DD 254 will be reviewed by OPNAV (DNS-34) and the program technical representative for currency and accuracy at least once every 2 years. Changes will conform to references (b), (c) and (k). All holders of the DD 254 will be provided any changes as soon as practicable. If there are no changes, and the DD 254 remains current, all holders will be notified in writing to that effect.

MAR 23 2009

CHAPTER 5
MARKING1. Basic Policy

a. OPNAV security serviced activities will adhere to the marking procedures of this chapter and chapter 6 of reference (b) when marking and classifying national security information. Strict application of marking requirements must be considered prior to marking classified documents. Classified material will be physically marked, annotated, or identified, as prescribed herein. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading and declassification actions. Therefore, all classified material must be marked in a manner that leaves no doubt about the level of classification assigned.

(1) Specific markings identify which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material. This requirement also applies to classified IT systems such as SIPRNET.

(2) OPNAV members must be aware that when individual items of unclassified information are combined, classification or higher classification by compilation may result. Paragraph 6-19, chapter 6 of reference (b) must be consulted for further details.

b. Classified material is any product of which the unauthorized disclosure could cause degrees of damage to national security. Where the word "document" is used in this instruction, it means publications (bound or unbound, e-mail, printed material, such as military reports, studies, manuals) correspondences (printed or written products such as charts, discs, maps, etc.). Most documents are easily marked, while other material, such as hardware, electronic media recordings, photography, etc., may be more difficult to identify because of physical characteristics. The markings identified at paragraph 2 below are required for all classified information, regardless of the medium by which it is revealed, with the following exceptions:

(1) An article that has appeared, in whole or in part, in newspapers, magazines or elsewhere in the public domain, will not be marked, controlled or restricted in any manner, while it

MAR 23 2009

is being reviewed and evaluated for comparison with classified information. The results of the review and evaluation, if classified, must remain separate from the article in question.

(2) Classified material will not be marked as prescribed in this chapter if the markings themselves would reveal a confidential source or relationship not otherwise evident in the material.

(3) A declassification date or event will not be applied to material which contains, in whole or in part, Restricted Data (RD) or Formerly Restricted Data (FRD). RD and FRD information will not be declassified without the prior approval of the Department of Energy (DOE).

(4) Classified correspondence to foreign governments or to their embassies, missions or similar official offices in the United States, will be marked only with the overall classification. Copies of the correspondence held by the originating office and disseminated to other commands must carry all of the required markings.

2. Basic Marking Requirements

a. Marking requirements and the application of markings vary, depending on the kind of material. Basic markings required for all classified material are:

(1) For originally classified material:

(a) The identity of the OCA (i.e., position title and office code).

(b) The agency and office of origin.

(c) The overall classification.

(d) The declassification date or event.

(e) Any downgrading instructions.

(2) For derivatively classified material:

(a) The source of classification (e.g., source document or classification guide), including its date when necessary for positive ID. If you derive classification from more than one source, use the phrase, "Multiple Sources." Keep

MAR 23 2003

a listing of the multiple sources with the file or record copy of a document or the related or accompanying documentation for other kinds of classified material. (Keep listing on file material.)

(b) The agency and office of origin.

(c) The overall classification.

(d) The declassification date or event. If you derive classification from multiple sources, carry forward the most remote date or event for declassification marked on any of the sources.

(e) Any downgrading action required.

b. Additionally, some material may require warning notices, intelligence control markings or distribution statements as described in paragraph 6-11 and exhibit 8A of reference (b). Derivatively classified material will carry appropriate warning notices or control markings from its sources that also apply to the new material.

c. Overall classification is the highest classification of any information contained in or revealed by the material. Overall markings are the overall classification, the most restrictive downgrading/declassification instructions applied to any information in the material and all warning notices or intelligence control markings applicable to the information in the material.

d. The classification authority, the office of origin, downgrading and declassification instructions, warning notices and intelligence control markings are collectively called associated markings.

e. Stamp, print or write classification markings in capital letters, larger than those used in the text of a document or conspicuously on other material, and, when practicable, colored red.

f. Classification and associated markings will be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal or similar device on classified materials other than documents, and on their containers. If the

1 MAR 20 2000

material or container cannot be marked, provide recipients with written notification of the classification and associated markings.

g. Mark major components of a document, which can be used independently, as individual documents. Examples are appendices and annexes to plans or operations orders. Enclosures to a letter of transmittal are always marked as individual documents. If an entire major component is unclassified, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and statement included such as "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method is used, no further markings are required on the unclassified major component.

h. Chapter 6 of reference (b) contains detailed guidance for marking documents. Exhibit 6A of reference (b) provides illustrations for markings of correspondence and other media, such as transparencies, sound recordings, etc. Exhibit 6B of reference (b) provides guidance on marking of classified U.S. Message Text Format (USMTF) messages.

i. An authorize listing of equivalent foreign security classifications by countries can be reviewed at reference (b), exhibit 6C.

3. Specific Marking Requirements for IT and Electronic Media. This includes film, photos, and discs, and can be reviewed further as follow:

a. Marking correspondence and letters of transmittals in accordance with reference (b), paragraph 6-25.

b. Marking of electronically transmitted classified messages in accordance with reference (b), paragraph 6-26, and exhibit 6B.

c. Marking classified files, folders and similar groups of documents in accordance with reference (b), paragraph 6-27.

d. Marking classified blueprints, schematics, maps and charts in accordance with reference (b), paragraph 6-28.

e. Marking classified photographs, photo slides, negatives, and unprocessed film in accordance with reference (b), paragraph 6-29.

MAR 23 2009

f. Marking classified briefings slides in accordance with reference (b), paragraph 6-30.

g. Marking classified motion picture films, videotapes and Digital Video Disc (DVD) in accordance with reference (b), paragraph 6-31.

h. Marking classified sound recordings in accordance with reference (b), paragraph 6-32.

i. Marking classified microforms in accordance with reference (b), paragraph 6-33.

j. Marking classified removable IT storage media and IT systems in accordance with reference (b), paragraph 6-34.

k. Marking classified documents produced by IT systems in accordance with reference (b), paragraph 6-35.

4. Working Paper Marking

a. Secret and confidential working papers will be marked with date when created and conspicuously marked centered top and bottom of each page with the highest classified level of information contained with the words "working paper" on the top left of the first page in letters larger than the text.

b. Top secret working papers will be marked the same as prescribed for a finished top secret document.

MAR 23 2009

CHAPTER 6
HAND CARRYING OF CLASSIFIED MATERIAL

1. Within a Command or Immediate Environs

a. When classified material is being carried within the OPNAV security serviced activities or its immediate environs (resident building) as part of normal duties, reasonable precautions, such as placing a cover-sheet over the material, will be taken to prevent inadvertent disclosure.

b. If the movement requires transportation other than walking, double-wrap and address the classified material. A briefcase may be considered the outer wrapping, except as noted in paragraph 6 below.

c. The requirements of chapter 10 of this instruction for wrapping, addressing and receipts, will be followed when classified material is hand carried to another command,

d. Contractor personnel are not authorized to hand carry classified material out of OPNAV security serviced activities spaces without prior arrangements and approval of OPNAV (DNS-34). With advance notice, OPNAV (DNS-34) will approve cases for periods of time up to 1 year to allow for multiple trips. In every case, hand carrying by contractor personnel will only be permitted if it is to the advantage of the Government. Each request will be handled individually and meet the requirements outlined in chapter 15, paragraph 5 of this instruction. A valid visit request meeting the requirements of chapter 14, paragraph 3 of this instruction, with company courier authorization for the contractor, must be on file. Requesting office must have also verified the contractor's clearance and access in JPAS and include a statement of such with the courier card request to OPNAV (DNS-34).

2. Procedures for Acquisition and Use of Courier Authorization Cards

a. DD 2501 Courier Authorization Cards are for use by individuals hand carrying classified material by means of surface transportation within a commuting area of the command. Security coordinators will submit requests for DD 2501s to OPNAV (DNS-34) via memorandum and e-mail.

b. OPNAV (DNS-34) will review all requests for DD 2501s and issue cards as justified. DD 2501s will be released to either

MAR 23 2009

the security coordinator or the individual courier. Security coordinators are responsible for maintaining accountability and control of DD 2501s issued under their cognizance to include retrieval of the cards when members detach from the command. DD2501s will be issued to individuals strictly on an "as needed" basis for a maximum of 1 year and must be returned to the security coordinator upon permanently departing the command.

3. Authorization to Hand Carry Classified Material in a Travel Status. Because of the security risk inherent in hand carrying classified material while in a travel status, OPNAV (DNS-34) will only authorize hand carrying when:

a. The classified material is required at the traveler's destination.

b. The classified material is not available at the command to be visited.

c. Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

d. OPNAV (DNS-34C) is the approval authority for hand carry of NATO materials as outlined in reference (f). For SCI material, approval must be obtained from OPNAV (N21).

4. Protection During Hand Carrying in a Travel Status. Personnel hand carrying classified material must be aware of the following:

a. The classified material must be in the individual's physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (continental United States only) is available. Hand carrying classified material on trips that involve an overnight stopover is not authorized without advance arrangements for proper overnight storage at a Government activity or at a cleared contractor facility. When package containing classified material is surrendered for temporary storage (e.g., overnight or during meals), the individual must obtain a receipt signed by an authorized representative of the contractor facility or Government installation accepting responsibility for safeguarding the package.

b. Classified material may not be read, studied, displayed, or used in any manner on a public conveyance or in a public place.

MAR 23 2009

c. When the classified material is carried in a private, public, or government conveyance, it will not be stored in any detachable storage compartment, such as an automobile luggage rack, aircraft travel pod or drop tank.

d. A list of all classified material carried or escorted by the individual will be maintained by his/her office; and upon his/her return, all classified material must be accounted for.

e. The individual will return the classified material to the office by any of the approved methods of transmission as stated in reference (b). If material must be hand carried, approval and documentation must be obtained from the command being visited.

5. Procedures for Obtaining Authorization to Escort or Hand Carry Classified Material on Commercial Passenger Aircraft

a. Because of the possibility of hijacking, classified material will be transported aboard commercial passenger aircraft only when other methods will not transport the material in time to meet operational objectives or contract requirements.

b. OPNAV (DNS-34) will approve hand carrying classified material aboard a commercial passenger aircraft upon receipt of a written statement authorizing the transmission signed by the cognizant security coordinator. This statement will include:

(1) The reason the material cannot be transmitted by other means;

(2) If there are overnight stopovers, state plans for overnight storage of classified material; and

(3) Include an itemized list of material to be hand carried.

c. The courier must have: a DD 2501; executed the "Classified Couriers Responsibility Acknowledgment" (exhibit 6A); and prepared for signature by OPNAV (DNS-34) an original letter on letterhead stationary authorizing hand carry of the material (exhibit 6B). The addressed outer envelop or container will be forwarded to OPNAV (DNS-34) for signature on the envelop or container on its face and for signature on the courier letter. The letter must contain the information as indicated at exhibit 6B.

MAR 23 2009

6. Procedures for Carrying Classified Documents Aboard Commercial Passenger Aircraft

a. A traveler carrying classified documents aboard a commercial aircraft will proceed through airline ticketing and boarding procedures in the same manner as all other passengers.

b. While traveling:

(1) The traveler must make sure the classified documents being carried have no metal bindings and are in double, sealed envelopes. (A briefcase or luggage cannot be considered as the outer container in this circumstance.)

(2) The traveler must present his/herself at the screening station for routine processing. If carrying the documents in a briefcase or other carry-on luggage, the briefcase or luggage will be routinely offered for opening for inspection. The screening official will then be able to inspect the envelopes by flexing, feel, weight, etc., usually without requirement for opening the envelopes themselves.

(3) If the screening official is not satisfied, inform the official that the envelopes contain classified material and exhibit an official DoD pass or military ID card, plus courier authorization. At that point, the screening official will process the envelopes with a detection device. If no alarm results, the envelopes require no further examination. If an alarm sounds, make arrangements with the security official to open the package out of sight of the general public to satisfy concerns. Contact the OPNAV Security Operations Center, (703) 697-3454 or 697-1310) during normal hours of 0700-1700, and the Navy Command Center, (703) 692-8883 after normal business hours. Follow procedures stated in the courier authorization letter.

c. Refer to paragraph 9-13 of reference (b) for more detailed procedures for carrying classified material in packages aboard commercial passenger aircraft.

MAR 23 2009

EXHIBIT 6A
S-A-M-P-L-E

CLASSIFIED COURIERS RESPONSIBILITY ACKNOWLEDGMENT

The following is a list of responsibilities under SECNAV M-5510.36 which apply to all authorized couriers of classified material:

1. Classified material must be in my physical possession at all times, unless under proper storage at a United States Government activity or an appropriately cleared contractor facility.
2. If necessary, overnight storage has been arranged with a Government activity or cleared contractor facility.
3. I will retain a receipt, signed by an authorized representative of the Government activity or contractor facility, upon surrendering classified material for overnight storage.
4. When classified material is carried in a private, public or government conveyance, I will not store it in any detachable storage compartments, such as automobile luggage racks, aircraft travel pods or drop tanks.
5. I may not read, study, display or use classified material in any manner on a public conveyance or in a public place.
6. A complete detailed list of the contents of the material to be transported has been left with a designated authority in my activity.
7. I understand that there is no assurance of immunity from search by security, police, customs, and/or immigration officials on domestic or international flights. If necessary, it may be opened out of sight of the general public.

I have read, fully acknowledge and understand my responsibilities as an authorized courier of classified material.

(DATE)

(SIGNATURE)

MAR 28 2007

EXHIBIT 6B

S-A-M-P-L-E

Date of issue

From: Chief of Naval Operations
To: To Whom It May Concern
Subj: COURIER AUTHORIZATION

1. Mr. John Thomas Doe (full name) of Chief of Naval Operations (name of activity) is authorized to hand carry three sealed packages, 9" X 8" x 24" (describe package(s) being carried) from Chief of Naval Operations, Pentagon, Washington, DC (addresser) to U.S. Naval Postgraduate School, Monterey, CA (addressee name) on 14 June 2007 (date)
2. Flight #59 departs National Airport at 1100 and arrives at (insert flight information including transfer points) Los Angeles International Airport at 1400.
3. Mr. John Doe (name of courier) will carry a DoD Badge #12345 (type of I.D. w/photo.) (If the courier is a civilian, include height, weight, date of birth and signature.)
4. This authorization expires 0900/07 June 1989 (Time/date not to exceed 7 days from date of issue.)
5. Confirmation of this authorization may be obtained by calling (703) 697-3454 or DSN 227-3454, M-F, 0700-1700, or (703) 692-8883, during abnormal hours, weekends and holidays.
6. This package contains classified material and is not to be opened in the general public under any circumstances. If it is necessary for the package to be opened and inspected, it is requested that the security agency assist with securing the package to the original state and sign the package after it is secured.

ALPHONSO W. MOORE
Director, Security Programs/
Command Security Manager

Copy to:
OPNAV (DNS-34)

117 2 8 2010

CHAPTER 7
ACCOUNTING AND CONTROL

1. Basic Policy

a. Classified information must be afforded a level of accounting and control commensurate with its assigned classification. Accounting and control measures will be implemented to limit dissemination, prevent unnecessary reproduction, determine the office or person normally responsible for the material's security, and determine holders so they can be notified of unscheduled changes in the classification or compromise of the material. In the case of top secret information, it is most important to keep a current record of page check, location of the information and a record of each individual whom the information is disclosed.

b. Common sense dictates that absolute accountability and control can only be assured for all classified information through a dedicated effort and total attention to regulatory details. It is also necessary to make distinctions in the degree of accountability and control and to set standards commensurate with the degree of damage to national security which might result from unauthorized disclosure of top secret, secret or confidential information.

c. The DoD mailroom has established procedures for screening of all incoming mail and packages via the Pentagon Remote Delivery Facility (RDF) and the Defense Post Office. For mail received by any other means, each OPNAV security serviced activity must establish screening points to ensure that all incoming mail and material delivered to offices under their cognizance are adequately protected until a determination is made whether it contains classified material. If incoming mail or material delivered to an office has not been screened and a determination has not been made as to whether it contains classified material, then the material may not be left unattended. This material must be secured in a security container when unattended until security determination is made.

2. Top Secret

a. The designated OPNAV security serviced activity's TSCO is responsible for receiving, maintaining accountability, distributing, reproducing and the destruction of all top secret material for OPNAV security serviced activities. Top secret

1702000

accountability and control procedures will be included in each OPNAV security serviced activity's internal security instruction.

b. All top secret documents originated or received by personnel must be turned over to the TSCO and entered into the accountability register. The register will completely identify the top secret document including changes, number of copies and disposition. The register will be retained for 5 years after the documents are transferred, downgraded or destroyed.

c. Each TSCO shall serially number all copies of top secret documents and each item of top secret equipment at the time of origination as follows:

"Copy no. _____ of _____ copies."

d. Top secret documents will contain a list of effective pages to be included in a "Record of Page Checks." When this is impractical, as in correspondences or messages, number the pages as follows:

"Page _____ of _____ pages."

e. The TSCO will page check top secret documents for completeness and accuracy on initial receipt and after entry of a change involving page entry or removal. This page check will be annotated on the "Record of Disclosure" and include the printed or typed name and signature of the individual performing the page check and date accomplished. (The change residue, including pages removed, must also be page-checked before destruction.) Page checks by the relieving officer, upon relief of a TSCO as custodian, are not required unless specifically directed.

f. Top secret documents will be physically sighted, or accounted for by examination of written evidence of proper disposition, such as certificate of destruction, transfer receipt, etc., at least once annually, and more frequently when circumstances warrant. At the same time, audit top secret records to determine completeness and accuracy. Procedures for conducting the top secret audit and inventory are located at exhibits 7A and 7B. Findings are reported as outlined at exhibit 7C.

MAR 23 2009

g. Retention of top secret documents will be kept to a minimum. Return top secret documents to the TSCO for destruction as soon as their intended purpose has been served. When top secret is destroyed, prepare a record of destruction identifying the material destroyed, the date destroyed, and the two officials who witnessed its destruction. Reevaluate top secret documents which cannot be destroyed and, when appropriate, downgrade, declassify, or retire them to designated records centers.

h. Account for top secret material by a continuous chain of receipts. Hand-to-hand transfer with signed receipts is required for internal distribution of top secret, with a record kept of each individual to whom the information is disclosed. Return top secret material to the TSCO for transfer outside of the command.

i. The TSCO will maintain a disclosure record for each top secret document revealing the document title, printed or typed name and signature of all individuals, including stenographic and clerical personnel, who have been afforded access to the document and the date of access. The TSCO shall retain OPNAV 5511/13 Disclosure Records for 2 years after the documents are transferred, downgraded, or destroyed.

j. Top secret material will only be reproduced by the TSCO and may not be reproduced without the consent of the originating agency or higher authority. Authority to reproduce will be obtained by the individual requiring the reproduction and forwarded with the top secret document to their TSCO for action. Annotate serially each copy produced.

3. Secret

a. Within the OPNAV security serviced activity, administrative security procedures will be established for controlling secret material to include records of material: (a) originated or received by the command; (b) distributed or routed to divisions or branches within the command; and (c) disposed of by the command by transfer of custody or destruction. The record may be in the form of a computer log, a mail log, a communications log, file of route slips, serial file or other administrative record.

MAR 23 2000

b. Signed receipts are not required for secret material that is distributed or routed within the command. Receipts are required when secret material accountability will be transferred from one command to another.

c. OPNAV security serviced activities may require additional controls for secret material as necessary for a practical balance of security and operational efficiency as documented by commands security standard operation procedures.

d. Transport or ship secret material by U.S. Postal Service (USPS) registered mail within and between the United States and its territories, or use of overnight domestic express delivery as directed at www.navysecurity.navy.mil. When mailing secret material, enclose a receipt identifying the document(s). This receipt must be signed and returned to the sender regardless of the method of transmission. The registered mail receipt does not replace the secret receipt. A registered mail receipt merely acknowledges that a package was received; it does not assure the sender that each piece of secret material has been entered into the accountability system of the recipient. The sending command is responsible for material until the addressee receives it. The sender cannot be sure that accountability has been transferred until the recipient signs and return the receipt.

e. OPNAV security serviced activities are not required to enter secret message traffic received through the Pentagon Telecommunications Center into accountability and control records. To safeguard messages and protect them appropriately to their level of classification, control internal routing through "need-to-know" and reproduce secret messages only per the requirements outlined in chapter 8, paragraph 1, of this instruction.

f. Refer to chapter 10 of this instruction for transmission of secret classified materials via SIPRNET.

g. For secret destruction accountability and record keeping, refer to chapter 12 of this instruction.

4. Confidential. There is no requirement to maintain records of receipt, distribution, or disposition of confidential material. Administrative provisions are required, however, to protect confidential information from unauthorized disclosure and compliance with the regulations on marking, storage, transmission and destruction.

MAR 28 2000

5. Secret and Confidential Working Papers

a. Secret and confidential working papers, such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain secret or confidential information shall be:

(1) Dated when created;

(2) Conspicuously marked, centered top and bottom of each page with the highest overall classification level of any information they contain, along with the words "Working Paper" on the top left of the first page in letters larger than the text;

(3) Protected per the assigned classification level; and

(4) Destroyed, by authorized means, when no longer needed in accordance with procedures outlined in chapter 12 of this instruction.

b. OPNAV security serviced activities will establish procedures to control and mark all secret and confidential working papers in the manner prescribed for a finished document when retained more than 180 days from the date of creation or officially released outside the command by the originator. A document transmitted over a classified IT system is considered a finished document.

6. Top Secret Working Papers. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers containing top secret information.

7. Special Types of Classified and Controlled Information. Control and safeguard special types of classified information as follows:

a. Naval Weapons Publication (NWP). Classified NWPs shall be safeguarded per this chapter, according to their security classification level. Administrative controls for NWPs do not replace classified information security controls.

b. NATO. Control and safeguard NATO classified information (including NATO Restricted) per reference (f).

MAR 23 2009

c. FGI. Control and safeguard FGI, other than NATO, in the same manner as prescribed by this chapter for U.S. classified information, except as follows:

(1) FGI control and safeguards may be modified as required or permitted by a treaty or international agreement, or by the responsible national security authority of the originating government for other obligations that do not have the legal status of treaty or international agreement (e.g., a contract).

(2) Top Secret FGI. Maintain records for the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmission of top secret FGI. The originating government shall approve reproduction, and destruction shall be witnessed by two appropriately cleared personnel. Retain records for 5 years per reference (l).

(3) Secret FGI. Maintain records for the receipt, internal distribution, transmission and destruction of secret FGI. Secret FGI may be reproduced to meet mission requirements and reproduction shall be recorded. Retain records for 3 years per reference (l).

(4) Confidential FGI. Maintain records for the receipt and transmission of confidential FGI. Other records need not be retained unless required by the originating government. Retain records for 2 years per reference (l).

d. RD (including CNWDI) and FRD. Control and safeguard RD and FRD per reference (g).

e. SCI. Control and safeguard SCI per OPNAV (N21)'s direction.

f. COMSEC. Control and safeguard COMSEC information per the OPNAV Electronic Key Management System (EKMS) manager.

g. NC2-ESI. Control and safeguard NC2-ESI per OPNAV NC2-ESI Control Officer (OPNAV (N5JA)) directions and in accordance with reference (m).

h. Special Access Program (SAP)s. Control and safeguard SAP information per reference (n).

i. Naval Nuclear Propulsion Information (NNPI). Control and safeguard NNPI per reference (o).

MAR 23 2009

j. FOUO. Control and safeguard FOUO information per reference (h).

k. Sensitive but Unclassified (SBU) Information. Control and safeguard SBU information in the same manner as FOUO, per reference (h).

MAR 23 2009

EXHIBIT 7A

S-A-M-P-L-E

TOP SECRET AUDIT AND INVENTORY

1. An inventory of all top secret material will be conducted at change of directorate TSCO, and at least once annually. Annual report is due to OPNAV (DNS-34) on 15 February each year. Change of directorate TSCO inventory report is forwarded to OPNAV (DNS-34) with the appointment notice as changes occur. (For change of directorate TSCO, relieving directorate TSCO will conduct the inventory.) At the same time, the top secret records are to be audited to determine completeness and accuracy. Publications distributed under the Communications Security Material System will be sighted and accounted for per EKMS-1. Inventory listing will include: control number assigned, copy number, originator, serial number, date, document title and/or subject.
2. Prior to conducting an inventory of top secret material, audit the records as follows:
 - a. Use the last inventory of holdings.
 - b. Add all incoming and outgoing material since the last inventory, as indicated by higher sequence control log sheets.
 - c. Delete the material transferred or destroyed since the last audit as determined by records of destruction, receipts, or completed control log sheets.
 - d. List the remaining documents as the audit top secret material accountable (for inventory) by the command.
3. The OPNAV security serviced activities' TSCO will provide any divisional ATSCOs with a list of their holdings (see exhibit 7B). The divisional ATSCOs will inventory the material held and report the results to the command's TSCO by memorandum. (See exhibit 7C.)
4. Inventory all top secret material listed in the current audit by physically sighting each document on the directorate inventories. The directorate TSCO will report the results of the inventory by memo to OPNAV (DNS-34).

MAR 28 2003

EXHIBIT 7B

S-A-M-P-L-E

TOP SECRET AUDIT AND INVENTORY

5511
Date

MEMORANDUM

From: Directorate Top Secret Control Officer
To: (Divisional) Assistant Top Secret Control Officer

Subj: DIRECTORATE TOP SECRET INVENTORY

Ref: (a) OPNAVINST 5510.60M

Encl: (1) Listing of Top Secret Holdings

1. According to my records, you have custody of the top secret documents listed in enclosure (1). Please conduct an inventory per reference (a) and report results via endorsed memorandum.

(Signature and date)

MAR 23 2009

CHAPTER 8
PRINTING REPRODUCTION AND PHOTOGRAPHY

1. Controls on Reproduction

a. Because there are so many reproduction machines throughout OPNAV security serviced activities' spaces, the problems associated with reproducing classified material have continuously grown. The convenience of reproduction equipment does not preclude obtaining the proper authorization needed for reproducing classified material.

b. Top secret information will not be reproduced without the consent of the originating activity or higher authority. All reproduction of top secret material will be accomplished only by the cognizance OPNAV security serviced activities' TSCO. Report all top secret reproductions to OPNAV (DNS-34) and ensure that reproduced documents are recorded and accounted for and included on command's annual inventory report.

c. OPNAV security serviced activities will designate officials (usually the security coordinators) who will approve requests to reproduce secret material. These officials have the responsibility to ensure that all classified reproduction requirements are observed and kept to an absolute minimum. Personnel within the command will be made aware of specific requirement and the approval process by the designated officials before reproducing classified material. It is recommended that designated officials be security coordinators.

d. Records will be maintained to show the number and distribution of all reproductions of top secret documents, classified documents covered by SAPs distributed outside the originating agency, and secret and confidential documents marked with special dissemination and reproduction limitations.

e. Specifically, designate the reproduction equipment authorized for reproducing classified material and prominently display signs on or near the equipment to advise users. Placards are available in the OPNAV Security Office, or the security coordinators can produce placards local as reflected at exhibit 8A. Reproduction machines should be located within areas that are easily observed to ensure that only authorized copies are being made and the number of copies are kept to a

MAR 23 2009

minimum. Only equipment under the control and use of the command's TSCO will be authorized for the reproduction of top secret material.

f. If the designated equipment involves reproduction processes using extremely sensitive reproduction paper, the paper will be used and stored in a manner to preclude image transfer of classified information.

g. Apply the same security controls to reproduced copies of classified documents as the originals.

h. Reproduced material must show the classification and other special markings which appear on the original material. Double-check all reproduced material and remark the reproduced copies that are unclear.

i. Safeguard any samples, waste or overruns resulting from the reproduction process, according to the classification of the information involved. Destroy this material promptly as classified waste. Check areas surrounding reproduction equipment for classified material that may have been left on nearby desks or thrown in wastebaskets. In the event the machine malfunctions, check to ensure that all copies have been removed. After reproducing classified material, make sure the original and all copies have been removed from the machine.

j. Reproduced copies of classified documents made with typical office copiers can leave legible images on the plastic surfaces of many three-ring and similar binders. The image transfers to the binder after the paper and plastic are in contact for some time. Classified document cover sheets should be used to preclude transferring the classified image to the cover of plastic binders.

k. If the reproduction equipment is networked to other IT systems or equipment, the whole network must be provided security protection and approved to process classified material at the highest level of classified material reproduced.

l. Before permitting un-cleared maintenance personnel access to or releasing reproduction equipment that has been used for processing classified material, inspect the equipment to ensure that no classified material has been left in the equipment.

MAR 23 2009

2. Tele Copiers. Tele copiers, facsimile equipment or similar devices using non-secure or unencrypted telephone lines will not be used to transmit classified information.

3. Requirement for Photography and Imaging Technology in Pentagon and Related NCR Facilities

a. The Pentagon and related DoD facilities in the NCR are prime targets for hostile intelligence collection and terrorist attacks. Advancing technologies have expanded the threat from small cameras and electronic imaging devices. Recent models of cell phones, for example, can transmit video as well as audio signals, making them in effect Video-Teleconferencing (VTC) instruments. Such "video-phone" features can compromise classified data and introduce major security risks.

b. Unless proper authorization has been obtained in advance from DoD or Service components occupying a space, the use of photographic or imaging device is forbidden in the Pentagon or DoD leased buildings. The following rules apply:

(1) Persons on official DoD photographic/video-graphic missions must use DoD authorized equipment.

(2) Members of such missions on DoD property must follow previously established ground rules.

(3) Cameras/imaging devices may be brought on/in those facilities, but used only with the permission of the component to which a space belongs. For permission in common areas or secured areas, contact PFFA at (703) 695-4668.

(4) Possession and use of a camera or imaging device in any area where collateral classified work is done requires specific permission from the security coordinator of that office.

(5) Possession and use of cameras or imaging devices in Sensitive Compartmented Information Facilities (SCIFs) are governed by even more stringent Defense Intelligence Agency (DIA) and Director of Central Intelligence (DCI) security policies. Consult the pertinent SCIF manager in advanced if such equipment is needed for mission accomplishment.

(6) Unauthorized use of cameras and imaging devices on/in DoD facilities can lead to loss, or suspension of security clearances, or more serious administrative and judicial action.

11/20/2010

(7) The officers of PFPA are empowered by their evidence collection duties to direct owners of cameras/imaging devices used in an unauthorized manner to remove and hand over the film or storage media in such equipment, or to conduct an on-the-spot review of the images just recorded.

(8) Persons sponsoring visitors to NCR facilities should advise visitors in advance about the strict control over the use of cameras/imaging devices.

c. These rules supplement DoD directives and the requirements of WHS Administrative Instruction (AI) No. 30, Security for the Pentagon Reservation, of 5 June 2002.

MAR 23 2009

EXHIBIT 8A

S-A-M-P-L-E

SIGN FOR POSTING AT REPRODUCTION MACHINE
(COLOR RED)

THIS MACHINE MAY BE USED FOR PRODUCTION
OF MATERIAL CLASSIFIED UP TO

SECRET

REPRODUCTION MUST BE APPROVED BY:

- ENSURE THAT ORIGINAL AND ALL COPIES ARE REMOVED FROM MACHINE PRIOR TO DEPARTURE
- ENSURE THAT CLASSIFIED MARKINGS ARE LEGIBLE. REMARK ALL DOCUMENTS ON WHICH THE MARKINGS ARE UNCLEAR
- IN THE EVENT THIS MACHINE SHOULD MALFUNCTION, CHECK TO ENSURE THAT ALL COPIES HAVE BEEN REMOVED

MAR 23 2009

CHAPTER 9
DISSEMINATION OF CLASSIFIED MATERIAL

1. Basic Policy

a. OPNAV security serviced activities will establish procedures for disseminating classified material originated or received by their offices, to limit outside dissemination to those activities having a "need-to-know" and to reflect any restrictions imposed by originators and higher authority. Procedures will be issued as a part of the command's internal security instruction required by chapter 1 of this instruction and will include, but not be limited to:

(1) As a minimum, an annual review of classified material distribution lists to ensure classified material is disseminated on strict "need-to-know" basis; and

(2) Request removal from distribution of unneeded classified material received.

b. OPNAV security serviced activities will ensure that material prepared for public release does not contain classified information or prescribed technical data. (See paragraph 8-7 of reference (b) for dissemination of technical documents.) Policies and procedures governing public release of official information and the circumstances under which security review is required are detailed in reference (p). Certain categories of information require review and clearance by the Assistant Secretary of Defense (Public Affairs) and are listed as exhibit 8B of reference (b). These categories of information are processed for public release under the procedures described in reference (p).

2. NATO Material. See reference (f) for guidance on dissemination of NATO information. DON documents incorporating NATO information and marked according to paragraph 6-16 of reference (b) do not require transmission through NATO channels.

3. Top Secret Material. Top secret material originated within the DoD will not be disseminated outside the DoD without the written consent of the originating department or agency, or higher authority. Members requesting dissemination out of DoD will provide the written consent to the cognizant TSCO with the request.

MAR 23 2003

4. Secret and Confidential Material. Secret or confidential material originated within the DoD may be disseminated to other departments and agencies of the Executive Branch of the Government unless specifically prohibited by the originator.
5. Dissemination to DoD Contractors. Information regarding the dissemination of classified material to DoD contractors is contained in chapter 15 of this instruction.
6. Disclosure to Foreign Governments and International Organizations. Authority for dissemination of classified information to foreign governments and international organizations is centralized at Navy Internal Program Office as outlined in reference (q). OPNAV security serviced activities will avoid entering into discussion with foreign persons or their representatives on initiatives that will result in the disclosure of Classified Military Information (CMI) or Controlled Unclassified Information (CUI) without first obtaining disclosure authority as outlined in reference (q). Additionally, personnel will avoid any actions that creates the false impressions that the Navy or U.S. Government is willing to enter into any arrangement with a foreign government leading to the eventual disclosure of CMI or CUI.
7. Dissemination to Congress. Information regarding disclosure to Congress is contained in paragraph 8-6 of reference (b).
8. General Policy for Dissemination of Intelligence
 - a. Authorized channels for dissemination of intelligence information have been established with the departments and agencies to comprise the intelligence community. The intelligence community composition is delineated in Executive Order 12333. Other channels for dissemination may be specified by DCI, in consultation with the National Foreign Intelligence Board, or as agreed to between the originating and recipient agencies. The intelligence community includes: Central Intelligence Agency (CIA); National Security Agency (NSA); DIA; special offices within the DoD for the collection of specialized foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; the intelligence elements of the military services; the FBI; the Departments of Treasury and Energy; the Drug Enforcement Administration; and staff elements of the office of DCI. The Director of Naval Intelligence (CNO (N2)) is the senior official

MAR 28 2013

of the intelligence community. The Office of Naval Intelligence (ONI), Suitland, Maryland, serves as dissemination authority and in-depth subject authority on behalf of CNO (N2).

b. The term intelligence means foreign intelligence and counter-intelligence and information describing U.S. foreign intelligence and counter-intelligence activities, sources or methods, equipment, and methodology used for the acquisition, processing, or exploitation of intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. intelligence collection efforts.

c. Any office desiring to disseminate intelligence requiring prior authorization by the originator, or in a manner contrary to the restrictions prescribed by the control markings in paragraph 6-12 of reference (b), must request permission from the originator via CNO (N2). Permission granted applies only to the specific purposes agreed to by the originator and does not automatically apply to any other recipient. Originators must give prompt consideration to these requests, particularly to reviewing, and editing as necessary, sanitized or paraphrased versions to derive at text suitable for release with lesser or no control markings.

d. DoD contractors may be provided selected intelligence when required in the performance of a DON contract unless specifically prohibited by reference (b) or this instruction. Intelligence will be released on a strict "need-to-know" basis. Authorization for release of intelligence to a contractor in the performance of a specific contract in no way implies authorization for release under another contract. Each release is treated separately, and authorization is required in each specific case, including release of revised editions of publications initially released. Commander, Office of Naval Intelligence (NIC-52) is responsible for execution of the policies on release of intelligence to contractors and is the final authority for determinations requiring refusal.

e. Violations of the restrictions and control markings prescribed in this instruction and reference (b) that result in unauthorized disclosure by one agency of the intelligence information of another, to which a DON command is a party, will be reported to CNO (N09N).

MAR 23 2009

9. Procedures for the Release of Intelligence to Contractors

a. When necessary for the performance of a DON contract, commands may release intelligence to DoD contractors without approval of NIC-52.

b. Prior to releasing intelligence to a contractor, the releasing office will:

(1) Ensure that dissemination is not prohibited by reference (b) or this instruction.

(2) Ensure that the conditions of reference (b) and this instruction are met prior to release.

(3) Ensure that all parts of the intelligence being released fall within the scope of the contract (as identified and supported on DD 254) under which requested. When all parts are not releasable, the releasing office will sanitize the intelligence information. (See paragraph 10 below).

c. The releasing office must maintain a record of all intelligence information released to contractors and report releases to the originator upon request.

d. Contracting officers will ensure that the requirements outlined in chapter 15 of this instruction are specifically included in the contract itself or on the DD 254.

10. Sanitization. The office releasing intelligence to a contractor is responsible for proper sanitization. If the releasing office is not aware of specific contractual commitments, coordinate release of the intelligence information to be released with those activities, which are able to determine the scope of the contract and "need-to-know" requirements of the contractor. Sanitization procedures for CIA documents will always include the deletion, from all CIA Directorate of Operations reports, of the CIA seal, the phrase "Directorate of Operations," the place acquired, the field number, the source description, and field dissemination, unless prior approval to release that information is obtained from CIA. Forward any requests for approval via NIC-52.

11. Prohibited Release

a. The following intelligence materials will not be released to contractors:

MAR 23 2009

- (1) National Intelligence Estimates (NIEs).
- (2) Special National Intelligence Estimates (SNIEs).
- (3) National intelligence analytical memoranda.
- (4) Interagency intelligence memoranda.
- (5) DIA Fact Book.

b. The following intelligence materials will not be released to contractors without approval of the originator, obtained through NIC-52:

- (1) Material which bears the following markings:
 - (a) "CAUTION PROPRIETARY INFORMATION INVOLVED (PROPIN)".
 - (b) "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON)".

- (2) Intelligence from foreign service reporting.

- (3) Intelligence materials which are marked for special handling in special dissemination channels (e.g., SCI).

c. Requests for authority to release material from foreign service reporting will be addressed to NIC-52 via the command sponsoring the contract for validation of "need-to-know," and include the following information:

- (1) Name of the DON contractor for whom the intelligence is intended.
- (2) Contract number on which the request is predicated.
- (3) Sponsoring contracting command.
- (4) Certification of contractor's facility clearance and storage capability for safeguarding classified material.
- (5) Complete identification of the material for which a release determination is desired.
- (6) Statement of justification confirming "need-to-know"

MAR 23 2000

and containing a concise description of that portion of the contractor's study or project which will confirm the "need-to-know" for the intelligence information requested. This statement is a prerequisite for a release determination.

MAR 28 2000

CHAPTER 10
TRANSMISSION OF CLASSIFIED MATERIAL

1. Basic Policy

a. Classified information will be transmitted either in the custody of an appropriately cleared individual or by an approved system or carrier, and per the provisions of this chapter and chapter 9 of reference (b).

b. The term transmission refers to any movement of classified information or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation - car, bus, train, ship, and plane - is not particularly significant.

c. The carrying of classified material across national borders is not permitted unless arrangements have been made for security, customs, postal, or other inspections. In addition, foreign carriers may not be used unless the U.S. escort has physical control of the classified material. (Refer to chapter 6 of this instruction for hand-carrying of classified material information.)

2. Top Secret. Top secret information will be transmitted only by:

a. The Defense Courier Service (DCS) - (refer to paragraph 17 of this chapter) for additional instructions regarding the use of DCS.)

b. Department of State diplomatic courier.

c. Cleared and designated U.S. military personnel or Government civilian employees traveling on a conveyance owned, controlled or chartered by the Government or a DoD contractor.

d. Cleared and designated U.S. military personnel or Government civilian employees by surface transportation. (See chapter 6 of this instruction.)

e. Cleared and designated U.S. military personnel or Government civilian employees on scheduled commercial passenger aircraft within and between the United States, its territories, and Canada, when approved per chapter 6 of this instruction.

MAR 23 2009

f. Cleared and designated U.S. military personnel and Government civilian employees on scheduled commercial passenger aircraft on flights outside the United States, its territories, and Canada, when approved per chapter 6 of this instruction.

g. A cryptographic system authorized by the Director, NSA.

h. A protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EMSEC) Issuance System. The Protected Wire Line Distribution System over which top secret information may be transmitted in unencrypted form will be considered for approval by Commander, Naval Information Operations Command, provided all of the following conditions have been met:

(1) All terminal equipment and connecting wire lines are installed per the appropriate RED/BLACK engineering and installation criteria.

(2) All end terminal equipment or subscriber sets are located in areas staffed only by personnel cleared for access to top secret information. All other personnel are excluded from the areas, except on official business, and then only under continuous surveillance or escort by top secret cleared personnel.

(3) Every effort is made to install connecting wire lines entirely within areas staffed only by top secret cleared personnel and where access is limited as described in subparagraph 2h(2) above. When this is not possible, those portions of the wire line which must be installed outside of top secret control areas must be under direct, continuing and complete control in order to preclude covert interception.

3. Secret. Secret information will be transmitted by:

a. Any of the means approved for the transmission of top secret, except that secret material may be introduced into the DCS only when U.S. control of the material cannot otherwise be maintained. Restriction on use of DCS does not apply to SCI and COMSEC material. When the Department of State courier system is to be used for transmission of secret material, the secret material shall be sent by registered mail to the State Department pouch room. The correct Navy addressing of the inner and outer envelopes for overseas activities is found in the

MAR 23 2009

Standard Navy Distribution List (SNDL), OPNAVNOTE 5400. As the SNDL lists the addresses for unclassified and classified mail, ensure address used is for receipt of classified material.

b. USPS registered mail within and between the United States and its territories.

c. USPS registered mail through Army, Navy, or Air Force postal service facilities, outside the area described in subparagraph 3b above, provided the mail does not pass through a foreign postal system or any foreign inspection, or via foreign airlines. The material must remain under U.S. control. Special care shall be exercised when sending classified material to U.S. activities overseas. If the material is introduced into a foreign postal system, it has been subjected to compromise. All mail to Fleet Post Office (FPO)/Army Post Office (APO) addresses outside the U.S. and its territories must be sent via registered mail.

d. USPS and Canadian registered mail with registered mail receipt between U.S. Government and/or Canadian Government installations in the United States and Canada.

e. USPS express mail for transmission between U.S. Government activities and between U.S. Government activities and contractors, within and between the United States and its territories. USPS express mail will not be used for transmission to an FPO/APO address.

(1) The use of USPS express mail is permitted when it is the most cost effective, risk managed method of transmittal, given the constraints of time, security and accountability. Because of the cost, use of the USPS express mail is not recommended by DON Headquarters mail centers and must be approved in advance. The use of Federal Express for transmittal of classified information is emphasized by the AAUSN Mail Center as an alternative.

(2) The USPS express mail and Federal Express envelope may serve as the outer wrapper. Classified material transmitted by both carriers will be prepared per subparagraph 3f below.

(3) Under no circumstances will the USPS express mail Form 11-B Waiver of Signature and Indemnity be executed for classified material. Likewise, block 7 of the Federal Express mail label may not be executed under any circumstances, including transmissions of confidential material.

MAR 23 2009

f. Designated express delivery holders of the GSA contracts for overnight domestic express delivery of secret and confidential material. See OPNAV (N09N2) Web site at www.navysecurity.navy.mil for updated listing. These services are prohibited for weekend delivery. Classified COMSEC, NATO, and FGI shall not be transmitted in this manner.

g. Electronically means over approved communication circuits to which safeguards have been applied to protect unencrypted classified information in accordance with references (b) and (r). OPNAV (DNS-34) will conduct physical security certifications and ensure that the Protection Distribution System certification is coordinated among OPNAV (DNS-4), OPTI and Commander, Naval Network Warfare Command.

4. Confidential. Confidential information will be transmitted by:

a. Any mean approved for the transmission of secret material; however, use of the USPS for confidential material is governed by the following:

(1) USPS registered mail will be used:

(a) For NATO Confidential;

(b) To and from FPO/APO addresses located outside the United States and its territories; and

(c) To other addresses when the originator is uncertain that their location is within the U.S.

(2) USPS first class mail will be used between DoD activities anywhere in the United States and its territories.

(3) USPS certified mail or, if required by subparagraphs 4a(1)(a) through (c) above, registered mail will be used for mail to DoD contractors or to non-DoD agencies of the Executive Branch. First class mail of confidential material is not authorized with markings of "return service requested."

(4) USPS express mail may be used between DoD activities and DoD contractors within the United States and its territories. However, because of the cost, use of the USPS

MAY 20 2000

express mail is strictly controlled within the DON and must be approved in advance by the Head, DON Headquarters Mail Center, or the Director, Secretariat Support Division, SECNAV.

(5) Certified or registered mail must be used when sending confidential mail to the State Department for forwarding by diplomatic pouch. If certified mail is not available, registered mail will be used.

b. In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens as outlined in chapter 9, paragraph 9-4 6., reference (b).

5. Telephone Transmission. Classified telephone conversations shall be permitted only over secure communication circuits approved for the classification level of the information being discussed. Every attempt shall be made to ensure that the classified information is not compromised to unauthorized personnel. All unclassified telephones will be labeled with "do not discuss classified information" markings.

6. Receipt Systems

a. Transmit top secret material under a continuous chain of receipts.

b. Forward secret material with a record of receipt, OPNAV 5511/10, between directorates, commands and other authorized addresses. Failure to sign and return the OPNAV 5511/10 receipt to the sender may result in a report of possible compromise or a command security violation report, OPNAV 5511/5.

c. OPNAV 5511/10 receipts for confidential material are not required except when the material is transmitted to a foreign government (including embassies in the United States). A receipt is required for all classified packages hand carried to the U.S. Senate.

d. The sender of the material will attach OPNAV 5511/10 to the inner cover. A sample receipt is exhibit 9B of reference (b). Receipt forms will be unclassified and contain only the information necessary to identify the material being transmitted. Top secret receipts will be retained for 5 years and secret receipts for 2 years in accordance with reference (1). When wrapping support is required by OPNAV (DNS-34), bring the receipt form to the security office during processing and wrapping of the outgoing classified material.

MAR 23 2009

e. When a page check document is included from the sender for classified publications, an additional receipt is not necessary.

7. Transmission to Foreign Governments. The transmission of classified material to foreign governments must meet the requirements of chapter 9, exhibit 9-A of reference (b).

8. Transmission of COMSEC Material. Transmission of COMSEC material per EKMS-1, Communication Security Material System (CMS) Procedures for EKMS (U), 5 October 2004.

9. Transmission of RD. Transmit RD documents (including CNWDI) and FRD in the same manner as other material of the same security classification per reference (s).

10. Transmission of SCI. Transmission of SCI per coordination with OPNAV (N21).

11. Transmission of SAP. Transmission of SAP in accordance with reference (n).

12. Transmission of NC2-ESI. Transmission of NC2-ESI in accordance with reference (m).

13. Transmission of FOUO and SBU. Transmission of FOUO and SBU in accordance with chapter 9, paragraph 9-5 of reference (b).

14. Consignor-Consignee Responsibility. For shipment of bulky material, complete in accordance with chapter 9, paragraph 9-7 of reference (b).

15. Classified Material Preparation for Transmission. Preparation of classified material for transmission will be done to protect it from unauthorized disclosure as outlined in chapter 9, paragraph 9-9 of reference (b)

16. Addressing of Classified Material

a. Classified material shall be addressed to an official Government activity or DoD contractor and not to an individual. An attention line may be used to include office code or department to aid in internal routing. The individual's name may appear on an attention line on the inner envelope. Consult with OPNAV (DNS-34C) for more details and support preparation for mailing classified material.

MAR 23 2009

b. Consult the following for complete and correct mailing addresses and mailing instructions:

(1) Current issue of the SNDL via Department of the Navy Issuance Web site (<http://doni.daps.dla.mil>) contains the official list of Navy fleet and mobile units, shore activities and their administrative addresses.

(2) The DSS, Industrial Security Facility Data, Facility Verification Request (DSS, ISFD, FVR) is the central activity for verification of DoD contractor facilities facility clearance, safeguarding capability and correct classified mailing address. The DSS ISFD FVR can be reached as follows:

Defense Security Service
ISFD FVR
2780 Airport Drive, Suite 400
ATTN: Customer Service
Columbus, OH 43219-2268

(3) A System Authorization Access Request (SAAR), DD 2875, with physical signature has to be signed and on file before gaining information from DSS. The DD 2875 will be scanned to a PDF file and e-mailed to account.request@dss.mil; the form can also be faxed to (614) 827-1544. Services by the ISFD can be improved by providing them with the Federal Supply or CAGE code of the DoD contractor facility. For questions with SAAR processing addresses or facility clearance, call 1-888-282-7682, option #1; then option #2, and again option #1. Written verification provided by the DSS ISFD FVR remains valid for a year from the date of issuance unless otherwise notified (superseded) in writing.

c. The inner envelope or container will show the address of the receiving activity.

d. An outer envelope or container will show the complete and correct address of the recipient and the return address of the sender.

e. Care must be taken to ensure that classified material intended only for the U.S. elements of international staffs or other organizations is addressed specifically to those elements and that the correct address for classified mail is used for overseas locations.

MAR 28 2009

f. When transmitting classified material through the Department of State mail facility for forwarding by diplomatic pouch through the Department of State courier system, the outer envelope will be addressed to Chief, Classified Pouch and Mail Branch, U.S. Department of State, Washington, D.C. 20520-0528. The inner envelope will be marked with the appropriate classification and addressed to the specific overseas activity.

17. DCS

a. The Secretary of the Air Force is the "DoD Executive Agent" for the DCS, and, as such, delegates and maintains a global courier network for the expeditious, cost effective distribution of highly classified and sensitive material as the Commander, Air Mobility Command. Operational control of global courier activities is exercised by DCS, Fort George G. Meade, MD, with a Pentagon substation operating out of the RDF.

b. Incoming: All Department of State material, including deadline delivery date material, will be picked up by the OPNAV, SECNAV, and Judge Advocate General (JAG) top secret control sections: OPNAV (DNS-34C), (703) 697-1156; SECNAV Administration Division, (703) 695-3822; and JAG-Code 11, Washington Navy Yard. DCS material is picked up from the RDF, Room 1J667B, 0800 to 1200 on Wednesdays. Only OPNAV (DNS-34) personnel who are listed on a qualified DCS Form 10 may pickup or deliver DCS material to the Pentagon substation. OPNAV (DNS-34C) will control and distribute DCS material as required.

c. Outgoing: The OPNAV, SECNAV and JAG top secret control sections are responsible for entering material into the DCS system per reference (t), and subsequent revisions.

MAR 28 2000

CHAPTER 11
SAFEGUARDING AND SECURITY STORAGE

1. Responsibility for Safeguarding

a. Members of OPNAV security serviced activities are responsible for safeguarding classified material at all times. This is particularly so for locking classified material in approved storage containers whenever it is not in use or under the direct observation of authorized persons. Only personnel with an appropriate eligibility determination and "need-to-know" are granted access to classified information or spaces. Personnel will also be aware of and follow procedures which ensure that unauthorized persons do not gain access to classified information by sight, sound or electronic means. Classified information will not be discussed with or in the presence of unauthorized persons.

b. Personnel will not remove classified material from designated offices or working areas except in performance of their official duties and under conditions providing the protection required by this instruction. (See also chapter 6 of this instruction on hand-carrying in a travel status.) Under no circumstances will personnel remove classified material from designated areas to work on during off duty hours, or for any other purpose involving personal convenience, without specific approval of OPNAV (DNS-34) or OPNAV security serviced activities' heads, as applicable. Approval will be given only when there is an overriding need, the required physical safeguards, including a GSA-approved storage container is provided, and a list of the material removed is kept at the command. Approval to remove classified material will not include permission for overnight storage without approval of CNO (N09N) as indicated in subparagraph 1c below.

c. Residential storage requirements will be forwarded via OPNAV (DNS-34) to OPNAV (N09N2) for chop and final approval by CNO (N09N). In all cases, a GSA approved safe will be available with intrusion detection system protection on sight. Written procedures will be also posted for classified material to be under personal control of an authorized member when removed from the security container.

d. Residential secure terminal equipment may be installed in a private residence when operational requirements are directed and cleared by the authorized EKMS manager, Navy Communications Security Material System (NCMS), Washington, DC.

MAR 28 2000

All residential installations are a privilege and may be suspended or revoked at anytime with notice. The following security requirement must be followed:

(1) The terminal must be used only by the person for whom it was installed.

(2) The KOV 14 card must be removed from the terminal following each use and kept in the personal possession of the user or stored in a security container approved for the classification level of the terminal's card.

(3) The terminal must be returned when requested by the EKMS manager, NCMS Washington, DC, for inventory or regularly scheduled maintenance. Failure to return the terminal when requested will automatically revoke this privilege.

(4) Prior to reassignment, retirement or transfer, the terminal must be returned to the EKMS manager. Failure to return this equipment is equal to theft of Government property.

(5) Immediately report the loss of a terminal or KOV 14 card to the EKMS manager, NCMS, Washington, DC.

(6) When communicating in the secure mode, ensure your location will not result in the compromise of classified discussions by eavesdropping.

2. Security Containers

a. General

(1) Classified material shall be protected by storage in containers authorized in chapter 10 of reference (b). The custodians' name shall be indicated on an SF 700 Security Container Information (see subparagraph 3d of this chapter) and posted on the inside of the container door or combination lock drawer. The custodian shall bear primary responsibility for compliance with security procedures relating to the container and its contents.

(2) No security container with wheels affixed is approved for storage of classified material. One-drawer containers must be fastened secure to prevent unauthorized removal.

MAR 23 2009

b. Control

(1) When new storage equipment is received, it will be coordinated through the SECNAV Lock Shop under OPNAV (DNS-34)'s guidance for inspection, numbering and combination setting.

(2) To ensure a complete and accurate inventory is maintained, no container will be moved from its assigned space without prior written approval of OPNAV (DNS-34).

(3) Requests for additional security containers will be submitted as follows:

(a) Via memorandum or e-mail to AAUSN, Facilities' Material Handling Unit. A written verification on each request will show a current physical security survey has been completed by OPNAV (DNS-34) including a review of on-hand security equipment and classified records for retirement, return, declassify or destruction. The memorandum shall include room number and type of container desired, as well as any further justification.

(b) Route the memo to AAUSN, Facilities' Material Handling Unit, carbon copying OPNAV (DNS-34).

(c) When the security container is delivered, the custodian must request a new combination change by calling the SECNAV Lock Shop (OPNAV (DNS-34)).

(d) After the combination is changed, the custodian will complete a new SF 700 with OPNAV (DNS-34) prior to close of business on the same day the combination is changed.

(4) Excess security containers shall be reported promptly to OPNAV (DNS-34). They must be returned as follows:

(a) Submit a memorandum to OPNAV (DNS-34). Ensure security container and room numbers are on the request.

(b) Remove all classified material.

(c) OPNAV (DNS-34) will change or request a contractor to change the combination to factory (50-25-50).

MAR 23 2009

(d) OPNAV (DNS-34) will respond to thoroughly inspect the security container and upon completion of the inspection, will notify AAUSN, Facilities' Material Handling Unit.

(e) The material handling unit will pick up the security container and return it to inventory.

(f) No security container will be placed in passageways.

(5) OPNAV (DNS-34) will be notified immediately should any doubt arise concerning the state of repair or suitability of any security storage equipment or open storage area. When problems arise and are not immediately reported, the possibility of lockouts or improperly secured containers may exist.

3. Combinations

a. Combinations will be changed when containers/locks are first placed in use (unless required more frequently by the type of material stored there), and when any of the following occurs:

(1) An individual knowing the combination no longer requires access.

(2) The combination has been subject to possible compromise or the security container has been discovered unlocked or unattended.

(3) The container (with built-in lock) or the padlock is taken out of service. Built-in combination locks will be reset to the standard combination: 50-25-50. Combination padlocks will be reset to standard combination: 10-20-30.

b. Combination change work shall be performed only by the SECNAV Lock Shop (OPNAV (DNS-34)).

c. When selecting combination numbers, sequential numbers (i.e., multiples of 5, simple ascending or descending arithmetical series) and personnel data, such as birth dates and SSNs, will not be used. The same combination will not be used for more than one container in any one open storage area or secondary control point. When setting a combination, numbers will be used that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

MAR 28 2000

d. After the combination is changed, the requesting office will submit a new SF 700 before the close of business on the same day the combination is changed. Copy 1 of the SF 700 will be affixed to the inside of the container on the combination lock drawer. To prevent a lockout, custodian should try the new combination before closing the container or vault door.

e. The combination of a secured area or container used for the storage of classified material will be assigned a security classification equal to the highest category of the classified material authorized to be stored in it.

4. Locking Procedures. The use of proper locking procedures, as outlined at exhibit 11A, when securing storage containers is vital to the protection of classified material. Security storage containers will be locked without haste, and re-checked. Use the following procedures:

a. Vaults, Map and File Safes. Firmly shut door or doors and rotate the combination dial at least four complete revolutions in one direction. Check and re-check.

b. Responsibility for securing is assigned to the custodian of each container. In the designated custodian's absence, an alternate custodian shall be designated and specifically charged with the responsibility for proper securing of the container.

5. OPNAV Locksmith Services. The SECNAV Lock Shop (OPNAV (DNS-34)) is responsible for all lock work involving room doors, combination locks on doors and security containers assigned. This responsibility includes those offices located outside the Pentagon in swing spaces, and other Metro Washington OPNAV and SECNAV assigned spaces. The SECNAV Lock Shop (OPNAV (DNS-34)) will provide keys for personnel within the Pentagon with the approval of the security coordinator. Lost, stolen, damaged or misplaced keys should be promptly reported to the SECNAV Lock Shop (OPNAV (DNS-34)).

6. Areas Protected by Electronic Alarm Systems

a. Electronic alarm systems may be installed in critical areas as a means of supplementing security storage equipment, but this protection is not intended to replace such equipment. Intrusion detection systems are designed to detect, not prevent, an attempted intrusion. Because of their cost, alarm systems are justified only when their use will result in a commensurate reduction or replacement of other protective elements without

MAR 28 2000

loss of protection effectiveness. Classified information located within alarmed areas shall be protected by the highest standard of security containers possible without detriment to the mission of the office concerned. Any deviation from this standard must be approved in writing by OPNAV (DNS-34).

b. Open storage of classified material must be limited to material up to and including secret in areas accredited for secret open storage. Open storage of top secret material is permitted only in areas presently accredited for top secret open storage. Open storage accreditation does not apply to any SAP material, such as NATO, NC2-ESI or CNWDI. An alarmed area approved for open storage shall be designated as a vault-type room and must conform to the following standards:

(1) Access door be secured with a built-in XO series three position, dial type, changeable GSA approved combination lock. One primary access door will be permitted in each alarmed area. This door shall be equipped with an automatic door closer and shall not be left open unless continuously manned and under direct observation of cleared personnel.

(2) All doors other than the primary access door must be secured with a positive lock or dead bolt from inside the area to prevent access by use of a key from the outside.

(3) All doors will be solid standard 1-3/4" (no vents or windows). Doors not solidly constructed must have proximity grid alarms to detect forced entry, as well as door switch alarms to indicate opening.

(4) Windows must be alarmed and will be permanently closed. Windows which might afford visual observation of classified activities must be made opaque or equipped with blinds, drapes or other coverings.

(5) All walls will be constructed from permanent material and extends from true floor to true ceiling or have an 18-guage expanded steel screen or an intrusion detection system installed to control openings of 96 square inches, including the space above the false ceiling.

(6) As an intrusion detection system's coverage of an area is fixed on installation, it may be greatly affected by changes in the area's physical structure. For this reason, area changes will be kept to a minimum. An impact assessment and possible reconfiguration of the alarm system may be necessary if

MAR 23 2009

alterations, construction or modifications are performed to an office layout. OPNAV (DNS-34) will be notified in advance to commencement of construction, modification, or alterations of an alarmed area.

d. When vacating an alarmed area, the custodian shall ensure the area is free of classified material and formally relinquish custody of the space by contacting AAUSN, Facilities' Material Handling Unit. While inspecting the area, particular attention should be paid to desks, filing cabinets, etc., left behind. On request of the custodian and contingent on availability of the SECNAV Lock Shop (OPNAV (DNS-34)), assistance will be provided to the custodian in sweeping the area for classified material. The custodian will turn over all keys and combinations to AAUSN, Facilities' Material Handling Unit.

7. Opening and Securing Alarm Areas

a. Access Lists. Personnel authorized to open or secure alarmed areas shall be identified in advance and approved by Pentagon Access Control. Refer to OPNAV (DNS-34) for specific procedures and requests for personal identification codes and space swipe access controls.

b. Securing Requirements. When the alarmed area is unmanned between the hours of 1800 to 0700 weekdays and at all times on weekends and holidays, secure the combination lock and set alarm system in "secure". Between the hours of 0700 to 1800 Monday through Friday, when alarmed areas must be unattended for 30 minutes or less, the combination lock must be secured and all non-primary entrance doors bolted shut. Between the hours of 0700 to 1800 Monday through Friday, when the alarmed areas must be unattended for more than 30 minutes, the combination lock must be secured, all non-primary entrance doors bolted shut, and the alarm unit set to secure.

c. Should difficulty be experienced when placing alarm system in access or secure, contact the Pentagon Alarm Monitoring Unit at (703) 697-8291, and state name, and area number being accessed or secured.

8. Unalarmed Work Spaces. After normal working hours, unalarmed spaces will be locked with a deadbolt lock. Electrically activated cipher locks do not afford the degree of protection required for classified equipment. These locks may be used during normal duty hours for access control purposes only.

MAR 23 2009

9. Care of Working Spaces

a. During working hours, to prevent access to classified information by unauthorized persons, monitor the entrance to office spaces and do not give un-cleared personnel freedom of movement within the office space. Escort visitors (including cleaning personnel) and question unescorted strangers found within the space.

(1) When classified documents are removed from storage for working purposes, they will be kept under constant surveillance, face down or covered when not in use. SFs 703 Top Secret (Coversheet), 704 Secret (Coversheet) and 705 Confidential (Coversheet) will be used to cover top secret, secret and confidential documents.

(2) Classified information will be discussed only when unauthorized persons cannot overhear the discussion. Particular care should be taken when there are visitors or workmen in the area.

(3) Preliminary drafts, carbon sheets, typewriter and printer ribbons, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information will be destroyed (placed in burn bag) by a method approved for destroying classified material immediately after they have served their purpose, or by giving them the same classification and safeguarding them in the same manner as the classified material they provided.

b. Top of security containers should be cleared of extraneous material, distinctive cover sheets should be used, and classified material should never be placed in desks. These measures will help prevent classified material from being intermingled with unclassified and overlooked when securing. If possible, all desks should be cleared when securing each day.

10. Security Check Lists

a. An SF 701 Activity Security Checklist shall be used and conspicuously posted in each room near the exit. SF 702 Security Container Check Sheet shall be posted on all security containers. Forms may be acquired per paragraph 6 of this instruction and held for reference for 1 year after the last entry.

MAR 23 2009

b. A division double-check procedure using a second person shall be employed wherever possible. Persons working late shall be listed as exceptions and are responsible for ensuring the security of their work area prior to departure.

c. OPNAV (DNS-34) physical security unit (703-693-9958 or 703-693-9429) will assist personnel securing their individual work areas, on an as available basis.

11. Key and Lock Control

a. General. Primary responsibility for key control rests with the space custodians, who will act as the key control officer for individual spaces. Each security coordinator will act as oversight for his/her organization and will be responsible to the key control officer for key control policy matters.

b. Responsibilities

(1) The key control officer is responsible to OPNAV security serviced activities for all security related key and lock control inventories, and will conduct an annual inventory of all keys and padlocks.

(2) Security coordinators will immediately inform the key control officer when unauthorized duplication or lost keys are discovered. Security coordinators will also inform the key control officer when office doors are replaced or removed. The security coordinators must ensure that original locks are either reinstalled or turned in to the key control officer. To facilitate recovery of keys when employees leave, security coordinators should ask supervisors to inform them when key holders give notice or receive Permanent Change of Station (PCS) orders. Security coordinators must also provide the SECNAV Lock Shop (OPNAV (DNS-34)) with notification of personnel authorized to check out a room key. It should be remembered that such personnel will have unlimited access to the office at all hours.

(3) The individual to whom a key is issued is responsible for both the key and for returning it to their security coordinator on request, when transferring or separating. All transfers of custody will be made through the security coordinator. Personnel will not loan their key to anyone or turn it over to their relief directly. Individuals must produce their keys at least once yearly to be inventoried. Personnel will report lost or defective keys and locks to their

MAR 23 2000

security coordinator. In the security coordinator's absence, contact the key control officer. Do not mark keys with information (name, room, office code) that might help unauthorized personnel use a lost key.

c. Key Control Records/Logs. Records maintained by security coordinators must show the number of keys on hand for each room, number issued, to whom, date/time of issue or return, and the signature of personnel checking out or returning security keys. Continuous accountability is required.

d. Issuance of Keys. Issuance will be determined by need. Convenience, rank or status is not sufficient criteria for issuance of a security key. OPNAV (DNS-34) is responsible for developing and enforcing rules governing key issuance and must approve any changes or exceptions to existing policy.

(1) Determination of which personnel within an office who receives keys should be made by the office's senior person or custodian.

(2) The SECNAV Lock Shop (OPNAV (DNS-34)) maintains a master key for all Navy spaces, which is available upon request for opening of spaces.

(3) Navy Reserve members should arrange for access to offices by coordination with their host office or activity. A security coordinator may place Reservists' names on a room's access list permanently or as needed for periods of entry.

e. Duplication of Keys. Security keys will not be duplicated except through the key control officer or security coordinator. Unauthorized duplication could result in administrative actions.

f. Alarmed Areas. Doors to alarmed areas will not be equipped with key locks. Alarmed area main access doors only require a built-in combination lock, dial type, changeable GSA approved combination lock. All non-primary entrance doors must be equipped with a 181 sliding dead-bolt on the inside of the door. These doors shall be used for emergency exit only. If a non-primary door must be opened temporarily (i.e., move furniture, carpet replacement, etc.), notify Pentagon Access Control of the situation.

MAR 23 2009

EXHIBIT 11A

S-A-M-P-L-E

PROCEDURES FOR SECURITY CHECK AT THE END
OF THE WORKING DAY

1. Each individual will ensure working area is secure at the end of the working day by:
 - a. Looking on top of, under, behind and in desks.
 - b. Making sure that working trays and baskets are empty.
 - c. Properly storing or shredding notes, rough drafts or similar working papers.
 - d. Placing classified documents, correspondence or related classified material in proper security containers.
 - e. Securely closing each drawer of the security container and locking the container by rotating the dial at least four complete turns in the same direction.
 - f. Checking the locking drawer to make sure the container is secured.
 - g. Surveying the general area to be sure nothing is unsecured. This includes looking on top of and in between security containers, general storage cabinets, working tables and checking trash cans.
2. Each week, a staff member will be assigned responsibility for double-checking the spaces to ensure that they have been secured, using the daily security checklist. Each item on the list will be checked and initialed. The double-checker will ensure that:
 - a. All security containers in the area are closed and locked by rotating the combination dial four times in the same direction and trying to open the locking drawer.
 - b. The disks and ribbons are removed from all printers and computer terminals.

MAR 23 2009

c. The reproduction machine is cleared by running it once and checking the reproduction paper for impressions. Machines will be turned off on weekends and holidays.

d. The shredder is cleared. The shred receptacle will be checked to ensure that the residue is from more than ten shredded pages.

e. The fax and copier are cleared.

f. Security container tops are cleared.

g. Individual office spaces are cleared.

h. Desk tops and trays are cleared.

i. Typewriter ribbons are removed from those machines using carbon ribbons, on which classified information has been typed.

j. Any electrical appliances are disconnected.

k. The general area is surveyed.

3. If anyone is still working in the area with a security container open, that person will then be responsible for securing the item, double checking, and initialing the checklist, showing the time of securing.

4. Each individual is responsible for performing the security responsibilities assigned. It is the individual's responsibility to arrange with the security coordinator for a substitute to perform the double-check when absence is anticipated. In the unplanned absence of the assigned double checker, the security coordinator will designate a substitute.

MAR 23 2003

CHAPTER 12
DESTRUCTION OF CLASSIFIED MATERIALS

1. General. The Director, WHS, Physical Security Division, promulgates policy for the destruction of classified material within the Pentagon, Navy Annex, Crystal City, Rosslyn and the Washington Navy Yard. As such, the Director directs the destruction of classified material through the Pentagon Incinerator Facility while developing procedures and scheduling the use of the facility. Specific schedules and questions may be directed to the incinerator facility at (703) 695-1828. Before destroying any record, classified or unclassified, the person carrying out the destruction process shall review part III of reference (1) to determine the lifecycle of the record about to be destroyed. No record shall be destroyed before its approved time. If emergency destruction is required when a state of war exists or is threatened, follow the guidance found in paragraph 5 of part I of reference (1).

2. Procedures

a. Classified material shall be placed in burn bags at the Navy office level. Commands are encouraged to have two persons responsible for transporting burn bags to the Pentagon RDF or pre-arranging for special pick up points as arranged by the incinerator facility. Burn bags are to be turned in at the Pentagon RDF between 0800 to 0900, or 1100 to 1200 daily.

b. All bags delivered to the RDF should be documented on a DD 2843 Classified Material Destruction Record. Bags are limited to being three-quarters full and no more than 10 pounds. Bags must be marked using a black marker to show office, point of contact, phone number and highest classification level of information in the burn bag, as well as the serial number (i.e., 1 of 3, 2 of 3, etc.). Also mark the bag containing personal data with "For Official Use Only (FOUO) - Privacy Sensitive - Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

c. Hard drives must be placed in a separate burn bag and identified as such. Limit hard drives to five hard drives per bag. Media, such as Compact Discs (CDs), cassettes or Video Cassette Recorder (VCR) tapes may be mixed in the burn bag with papers. No trash, metal or glass is allowed in burn bags! Burn

MAR 28 2000

bags must be protected and stored in areas out of view from the office entrance doors at all times until delivered to the RDF for destruction.

3. Destruction Reports. Although the use of OPNAV 5511/12 Classified Material Destruction Report is no longer required by reference (b), all personnel will record the destruction of secret and above material for documentation. History indicates that record keeping on destructions provides documentation for future reference.

a. The cognizance directorate TSCO or alternate shall accomplish destruction of top secret material. They must record destruction of top secret and special types of classified information by any means as long as the record includes complete identification of the information destroyed and date of destruction. Two witnesses should execute the record when the information is placed in a burn bag or actually destroyed. Top secret destruction records must be retained for 5 years.

b. Records of destruction are not required for secret and Confidential information except for special types of classified information (see chapter 10 of reference (b)). In cases where the originator states that a document "may be destroyed without report," the originator does not need to know the document was destroyed. However, a record of destruction is still good practice; maintain for minimum of 2 years when done.

4. Message Traffic

a. Unclassified message traffic, except NNPI, does not have to be destroyed as classified material. Offices with high volumes of classified and unclassified message traffic may destroy all messages through use of burn bag to ensure efficient handling and to preclude inadvertent disposal of classified material. FOUO messages will be destroyed by tearing each copy into pieces to preclude reconstruction, and placing them in burn bag to provide protection for any sensitive subjects or personal data and to preclude public disclosure of Privacy Act data as outlined by reference (h).

b. The requirement for recorded destruction of routine short life secret message traffic received from the Joint Communication Center (JCC) has been waived because of the high volume of message traffic. Classified messages are distributed via SIPRENT by the JCC to customer per established restricted

MAR 23 2009

profile to individuals vice public folders. Secret messages must still be destroyed by authorized means through burn bag use or shredding and by authorized persons.

5. Destruction of CMS Material. COMSEC and other CMS material will be destroyed by designated command EKMS personnel, under NCMS, Washington DC, using the SF 153 COMSEC Material Report in accordance with EKMS-1, CMS Policy And Procedures for EKMS (U), 5 October 2004. Completed SF 153 must be turned in to the CNO EKMS Manager, Naval Communications Material Security, Washington, DC.

6. Emergency Action Procedures

a. Mass destruction or total removal of classified material is not considered feasible within OPNAV security serviced activities. The following instructions govern emergency action procedures for the protection, removal, and destruction of classified material during a fire, natural disaster, civil disturbance, or enemy action.

b. Emergency procedures will be implemented at the direction of the Director, PFFPA, or GSA building manager via Computer Based Emergency Notification System (CENS) or "Big Voice" intercom announcements. In the event of the absence of the above, the senior individual present will direct emergency procedures. For those personnel not physically located in the Pentagon, emergency procedures are established by the occupant emergency official and building manager.

c. Procedures. Upon receipt of implementing instruction:

(1) Classified material will be returned to authorized security containers which will then be locked and left in place.

(2) Personnel will remain at duty position pending receipt of further instructions.

(3) In the event of natural disaster (i.e., storms, earthquake, or fire, etc.), necessitating evacuation of personnel, classified material will be secured in authorized storage containers.

d. Destruction. OPNAV security serviced activities physically located within the Pentagon are exempt from the emergency destruction of classified material. Offices not located in the Pentagon need to establish priorities of

MAR 23 2009

emergency/destruction which are consistent and relative by level of classification (i.e., Priority 1: Top Secret, Cosmic Top Secret Atomal and Cosmic Top Secret; Priority 2: U.S. Secret, NATO Secret Atomal and NATO Secret; Priority 3: U.S. Confidential, NATO Confidential Atomal and NATO Confidential; Priority 4: FOUO, U.S. Unclassified requiring operations security protection , NATO Restricted, and NATO Unclassified). COMSEC, codeword, and special access material are prioritized accordance to security classification levels.

e. Relocation. Relocation will generally be limited to the relocation of personnel and material required for operations in accordance with contingency plans.

f. Safety. In the implementation of above procedures, the personal safety of individuals must not be jeopardized.

g. Guards. PFPA is responsible for protection of the Pentagon, its occupants and Government and private property. OPNAV (DNS-34) interfaces with PFPA and, in consonance with guidelines, administers security enforcement procedures within OPNAV security serviced activities through the security coordinators.

h. Reports. Post reporting is required in the event of any emergency. Reporting will include all details surrounding the emergency, including extent of compromise and possible compromise, as applicable. Reporting will be accomplished without delay, through command channels to CNO (N09N). Format contained in reference (b), paragraph 12-8, will be followed relative to compromise and possible compromise and possible compromise situations, report symbol OPNAV 5510-6B applies per reference (b), appendix C).

i. Post copy of emergency action procedures correspondence within work areas and alert all personnel during annual security refresher training.

MAR 23 2009

CHAPTER 13
OPNAV SECURITY SERVICES

1. Pentagon Parking Program. This chapter assigns responsibilities and describes general requirements and procedures for OPNAV security serviced activities' input to the Pentagon Parking Program via the AAUSN parking officer. OSD AI No. 88, 26 June 1989, provides detailed regulations for parking, vehicle operations and pedestrian traffic on the Pentagon Reservation, Arlington County, Virginia. With exception of parking identified at paragraph 6.c.2, this chapter, all vehicles parked on the Pentagon Reservation will have parking pass, parking clearance, or be subject to towing.

2. Authority. The Director of PFPA is assigned overall responsibility for the implementation, operation and control of the Pentagon Parking Program. OPNAV (DNS-34) coordinates OPNAV's parking requirements via the DON parking office, AAUSN's Facilities Division, as the OPNAV parking control officer.

3. Responsibilities

a. DNS. Administer requirements delineated by AI No. 88 for OPNAV members, and develop a viable parking program throughout OPNAV. Pentagon parking is not available to OPNAV members that are receiving metro-subsidies for travel to work.

b. OPNAV security serviced activities. Each activity will appoint a parking coordinator and an alternate to administer internal responsibilities; names, room numbers, and telephone extensions will be submitted in writing to OPNAV (DNS-34).

c. OPNAV parking control officer, OPNAV (DNS-34). Serves as liaison between OPNAV, SECNAV and PFPA Central Parking Office on requirements; allots parking passes ("C", "A") to activity based on on-board personnel and command need; and monitors implementation of parking program while assisting the activities in developing and maintaining internal assignment of allotments.

d. The OPNAV security serviced activities parking coordinator is responsible for determining whether requests for "C" and "A" passes meet regulation, and approve requests based on their allotment while ensuring information regarding assigned permits is kept up to date. The parking coordinator will also retrieve passes from individuals who detach from OPNAV security serviced activities, as "C" and "A" passes are not transferable between members without proper database documentation.

MAR 28 2003

4. Assignment of Parking Permits. The allocation of "A" and "C" passes assigned to each activity is based on the number of on-board personnel working in the Pentagon (including swing spaces) and the number of personnel whose work assignments meet the following parking criteria:

a. General Parking. "C" permits are assigned to on-board employees working in the Pentagon, or employees who work unusual hours or rotate shifts (shift workers), and are based on personnel with job requirements certified to warrant "C" parking assignments. The employees shall be employed and physically working in the Pentagon. "C" parking permits shall not be awarded based on rank/grade, position, or job title.

b. Executive Parking. "A" parking allocations are intended for flag officers, SES, O-6 and YC-3. "A" passes will be allocated proportionately to each OPNAV security serviced activity, based upon senior manning strengths.

5. Physically Disabled Parking. A number of parking spaces are reserved for employees certified as physically disabled. Requests shall be initiated by the individual, and will include sufficient detailed documentation from a physician for coordination with DiLorenzo Tricare Clinic for further medical examination. Such individuals shall physically work in the Pentagon. When the handicapping condition is temporary, state the length of time a permit will be necessary. Expired or permanent permits that are no longer needed must be turned in to the activity's parking coordinator. Processing for a physically disabled parking permit is as follows:

a. Military Personnel. All physician statements in support of physically disabled parking requests shall be submitted by the employee directly to the Dilorenzo Tricare Health Clinic, room MF859D-100 (corridor 8). Upon receiving a favorable medical evaluation, a request for a physically disabled parking permit will be via a DD 1199 Pentagon Reservation parking Permit Application. The DD 1199, accompanied by supporting statements from the Dilorenzo Tricare Health Clinic, will be submitted via the employee directly to the Pentagon Parking Office.

b. Civilian personnel. All physician statements in support of physically disabled parking requests shall be submitted by the employee directly to the Pentagon Civilian Employee Health Service, room MF859D-100 (corridor 8). Upon receiving a favorable medical evaluation, a request for a physically

MAR 28 1999

disabled parking permit shall be made by completing a DD 1199. The DD 1199, accompanied by supporting statements from the Pentagon Civilian Employee Health Service, will be submitted via the employee directly to the Pentagon Parking Office.

6. Visitor Parking

a. Corridor 5, Mall and River Plazas parking spaces are reserved at all times and require prior clearance by the AAUSN parking coordinator. A 2-hour limit is placed on the use of these spaces and is applicable 24 hours a day, 7 days a week, including holidays. When visitors authorized to park in these areas must overstay the time limit, requests for extensions must be processed through the AAUSN parking office, (703)697-0874, before the end of the original 2-hour time limit.

b. Mall Annex Parking Lot (Very Important Persons) requirements are the same as Mall and River Plazas with the exception of visitors who will be here for longer than 2 hours. Individuals in the grades of SES, general or flag officer rank, or personal visitors to OPNAV security serviced activities, may also park in the Mall annex parking lot. Clearances must be called in to the AAUSN parking office at (703)697-0874.

c. Visitors parking lanes (South 26/North 43) are reserved in advance via the OPNAV (DNS-34) and provided for general visitor parking and are reserved exclusively for bona fide visitors to senior flag and SES officials in the Pentagon. Lane 26 parking is located in south parking north of corridor 3 while lane 43 is located in north parking south of the River entrance. Clearances must be called in to OPNAV Security office at (703)693-9458.

(1) The visitor lanes will be open 24 hours a day on normal Government work days for official visitors. Pentagon occupants are not authorized to park in these lanes.

(2) Visitor parking is also available for the general audience and pentagon occupants without a parking permit on Fern or Hayes Streets between the hours of 1700 and 0700, daily, weekends and holidays.

7. Car Pool Parking. Those employees desiring to use car pools should direct all questions to the Pentagon Parking Office, (703) 697-6251, located on the concourse near the Post Office to apply for "B" permits. Car pool applications are not coordinated via the DON parking coordinator, nor OPNAV (DNS-34).

MAR 23 2009

8. Parking Regulations. General responsibilities of the parking permit holder and/or car pool members are:

a. Keeping all car pool information current. Failure of the principal member to update changes as they occur, or within 10 working days, shall result in the revocation of parking privileges. A new permit may be issued without a waiting period based on the number of valid car pool members.

b. When parked at the Pentagon, display the parking permit on the vehicle rear view mirror so that the permit number is plainly visible and readable through the vehicle windshield.

c. Permits for duty officers, unmarked Government-owned or leased vehicles may be transferred for legitimate purposes but not for circumventing the parking procedures.

(1) Individual parking permits are non-transferable.

(2) Car pool permits are transferable among registered car pool members only.

d. Parking permits are Government property and must be returned to the Pentagon Parking Office immediately on canceling, invalidating, transferring of the holder, or dissolving of a car pool.

e. Vehicles are subject to towing when they are covered with any type of car cover prohibiting officer from readily seeing the permit number. PFPA shall not be responsible for removing covers to view parking permits.

f. Safeguard your permit, as the number of replacement of lost, stolen or damaged permits is limited by the Pentagon Parking Office.

g. Permit holders may not park in excess of 18 hours in one location unless prior written request from a valid individual permit holder for such extended parking is approved by the Pentagon Parking Office via OPNAV (DNS-34).

h. Parking in marked parking spaces. Parking in other than designated parking spaces, on the grass areas, along yellow curbs, blocking or partially blocking traffic or pedestrian lanes is prohibited. Oversized vehicles (too large for the designated parking space) are prohibited and subject to a violation notice, or towing.

MAR 23 2009

i. Flagrant violations, such as falsifying applications, counterfeiting, altering, or reproducing permits, failing to turn in car pool permits when the car pool membership changes, receiving more than one parking violation notice in a 12-month period, and any act circumventing the regulations to gain favor, shall result in the loss of the privilege to park for at least 6 months. The revocation shall apply to all parking areas and shall be handled by OPNAV (DNS-34).

j. Under no circumstances shall parking permits be copied, altered, or duplicated. Possessing such permits shall result in legal action by PFPA and administrative action by the Pentagon Parking Office.

k. No person shall park a motor vehicle in the parking areas or roads of the Pentagon Reservation contrary to governing regulations or to the directions of posted signs.

l. The lawful orders and direction of PFPA officers must be followed at all times.

9. DD 2501 Courier Cards. Are issued by OPNAV (DNS-34) as indicated below.

a. General courier cards should be requested through the divisional security coordinator. The security coordinator will submit a request for a courier card after verifying the requesting member has a valid investigation to match requested level of clearance. The security coordinator will submit a request on letterhead with the following information: name, rank, SSN, and clearance level requested. The requests should be faxed to (703) 614-4399, or hand delivered to OPNAV (DNS-34).

b. Issuance. The requested courier card will be issued to the named member or the security coordinator of the named member.

10. Fingerprinting Procedures

a. OPNAV (DNS-34) has the capability to conduct electronic fingerprints for the purpose of security investigations, law enforcement requirements, and to assist in screenings for positions involving adolescents.

b. To request fingerprint services, contact OPNAV (DNS-34) at (703) 693-9458. Fingerprints will be electronically taken

MAR 28 2003

with the IDENTIX Touch print 3000 Live Scan fingerprint machine. The prints will be printed out on SF 87A Finger Print Chart and either provided to requesting member or forwarded to OPM for processing with appropriate security investigation request.

MAR 28 2000

CHAPTER 14
VISITS AND MEETINGS

1. General

a. Basic policy regarding visits and meetings is found in chapter 11 of reference (b). Upon arrival, visitors must check-in with the command's security coordinators for initial briefing and further guidance.

b. For security purposes, the term visitor applies to:

(1) Any person who is not permanently attached by PCS orders, or a civilian DD 2918, National Security Personnel System Position Description, or employed by the command.

(2) Personnel on temporary additional duty.

(3) Reservists, stashes, detailed Inter-governmental Personnel Act (IPA), concessionaires and contractors are also considered as visitors (appointed senior IPAs are treated as permanent employees).

(4) Un-cleared members and support staff including cleaning personnel, movers and repair technicians are visitors requiring escort, and movement shall be controlled and escorted at all times to ensure that access to classified information is not disclosed. Be particularly mindful of assigned Government personnel designated to test and penetrate command's security posture for training purposes.

c. JPAS is the DoD's official system of record for visit classified requests. Under no circumstances may personnel hand carry their own visit request(s) as proof of clearance.

2. Outgoing Visits

a. CNO has directed the use of JPAS for personnel security administrative functions, including the administration of visits involving access to classified information. Use of OPNAV 5521/27 Visitor Request is not required but used minimally as commands continue to field the electronic JPAS capability. When the OPNAV 5521/27 is used, it will be completed as proof of clearance for classified visits by OPNAV security serviced activities personnel. Security coordinators or ASCs will verify accuracy of JPAS data and OPNAV 5521/27, and in the case of the latter, sign and mail or fax visit requests to appropriate host

MAR 28 2000

activities. Visit requests transmitted via electronic mail must be transmitted from the command security manager to the attention of the security manager of the command or DoD contractor facility to be visited.

b. Security coordinators or ASCs sponsoring the visitor are responsible for ensuring and validating the accuracy of the access and affiliated data in JPAS before initiating the visit request. JPAS database issues will be coordinated with OPNAV (DNS-34B). The visited command releasing classified information is responsible for verifying "need-to-know" and for positively identifying the visitors. In addition to requirements for authorizing access to classified information, the visited command must also fulfill the local facility access and general visit control requirements. If local conditions necessitate formal visit request letters for visit/access control purposes, the command sponsoring the visitor must comply with local facility access requirements. Visit requests submitted through JPAS will not be accepted if they do not reflect accurate access documentation including the "Nondisclosure Agreement and accurate affiliation documentation including appropriate point of contact and Security Management Offices (SMO) information.

3. Incoming Visits

a. OPNAV (DNS-34) is the central point for policy and direction on incoming visit requests from all outside activities. Commands receiving visit requests directly will only forward them to OPNAV (DNS-34) to document requirement for building badges.

(1) OPNAV security serviced activities receiving visit requests from other DoD activities or Government organizations will process and file them appropriately for documentation of clearances, access and building passes.

(2) Visit request files are subject to periodic commands security inspection by OPNAV (DNS-34).

(3) Incoming visit requests from contractor facilities must meet the same JPAS or other electronic documentation as Government personnel.

b. Before access to classified information may be granted to a visitor, the host office must:

MAR 23 2009

(1) Check visitor ID (i.e., Government/contractor picture ID badge or drivers' license).

(2) Have on file a valid visit request with the visitor's security clearance endorsed by either OPNAV (DNS-34) or command's security coordinator.

(3) Refer to chapter 15 of this instruction for in-depth information regarding access and classification specifications by contractor personnel.

4. Visits to DOE Activities

a. DOE Request for Visit or Access Approval, DOE F5631.20 Form, will be completed for visits to DOE activities and related contractors. The initiating office will forward to OPNAV (DNS-34) the completed form, including a typed addressed envelope or fax phone number, 3 days in advance to allow sufficient time for processing including faxing and mailing.

b. The "To" address block will be filled in with the address of the appropriate DOE activity or contractor facility, unless the visit requires access to weapons related RD or CNWDI. In such cases, the requesting office will leave the "To" block and the accompanying envelope blank, to be completed by OPNAV (DNS-34).

c. Access certification, briefing and debriefing requirements of chapter 2, exhibits 2C through 2G, of this instruction must be met prior to forwarding visit requests for CNWDI and RD accesses. Reference (g) applies.

5. Visits by Representatives of the Government Accountability Office (GAO). Properly cleared and identified representatives of GAO may be granted access to classified DON information in the performance of their assigned duties and responsibilities per paragraph 11-5 of reference (c).

6. Visits by Foreign Nationals

a. Policy and procedures for classified or unclassified visits by foreign nationals are described in detail in reference (q). Policy and procedures for visits of nationals from communist controlled countries are contained in reference (u).

b. Visits by foreign nationals, including foreign temporary exchange officers, which will involve substantive technical

MAR 23 2009

discussions or the disclosure of classified information require the approval of the Navy International Programs Office (IPO-01B2). Coordination with Navy Foreign Liaison (OPNAV (N2L)) is required for issuance of building passes. Exchange officers program must comply with condition of DoD Directive 5230.20 of 22 June 2005. A copy of the personnel exchange agreement will be provided to OPNAV (DNS-34).

7. Classified Meetings

a. Any meeting which will involve the disclosure of classified information must be held at a Government installation or cleared DoD contractor facility where adequate physical security and procedural controls have been approved.

b. See chapters 7 through 13 of reference (b) for detailed responsibilities for security sponsorship of classified meetings, conferences, seminars, symposiums and conventions, specific security procedures for classified meetings and procedures for obtaining clearance for non-government attendees.

c. All requirements for top secret meetings or meetings at base theatres, school auditoriums and in secured classrooms will be coordinated with OPNAV (DNS-34). Further coordination of Technical Surveillance Countermeasures (TSCMs) support is in order. DON security regulations specifically state that classified meetings may not be held at hotels, conference centers or any other non-cleared facility.

d. Conference Rooms

(1) Protection of classified information within a conference room is the responsibility of the official sponsoring the meeting. Prepare a security plan to minimize risk and to promulgate and manage classified documents and discussions in accordance with reference (b).

(2) The official with requirement to hold a top secret meeting in a conference room which is not alarmed will notify OPNAV (DNS-34) at least 30 working days in advance so that a TSCM can be scheduled and conducted.

(a) Requests for TSCMs should state specific room number and date of meeting and will be classified secret. Declassification statement to be placed on the request is:

MAR 23 2009

"Classified by OPNAVINST 5513.4E, ID 04-17,
Declassify (as marked on the source/event and dated)."

(b) Upon completion of the survey, the official sponsoring the conference is responsible for providing access control of the conference area until the conference is over.

(3) Meetings classified secret or above require a monitor while the conference is in session. Monitors must have a security clearance equivalent to the classification of material to be discussed. They must provide access control by ensuring that personnel attending the conference have clearance equal to or higher than level of information to be discussed and a "need-to-know."

(4) Telephones located in conference rooms shall be disconnected or batteries removed at all times.

8. Unclassified Meetings

a. Material prepared for presentation at unclassified meetings and instructional courses on subjects concerning sensitive research, SBU information, and operations should be submitted for security review.

b. Guidance as to categories of information requiring review and the administrative procedures for submitting the information for review are found in reference (p).

MAR 28 2003

CHAPTER 15
INDUSTRIAL SECURITY

1. General. The security of the United States depends in part upon proper safeguarding of classified information implemented by and released to industry. Classified information is the property of the U.S. Government. It may be provided to private industry only in connection with a bona fide contractual requirement. Reference (k) provides the contractor with the minimum safeguarding requirements for classified information; it does not provide security classification guidance.

Classification guidance is provided to the contractor in the DD 254. The DD 254, with its attachments, supplements, and incorporated references, is the only authorized means for providing security classification guidance to a contractor in connection with a classified contract. Only the procuring military department may originally classify information. A contractor merely marks and protects that information developed under a contract on the basis of the DD 254 issued by the Government User Agency (UA). The UA is the command which actually conducts the contracting process. The UA is responsible for providing contractors all security classification guidance necessary to properly classify information and material produced under the terms of the contract. It is essential that comprehensive classification security guidance be furnished to contractors. The overall DoD responsibility for administering the Industrial Security Program is assigned to the Director, DSS.

2. Classified Contracts. A classified contract is one which requires or will require access to classified information by the contractor (or employees) in the performance of the contract. A contract may be classified even though the contract document itself or task is not classified. A DD 254 shall be prepared following the provisions of exhibit 15A by the cognizance program office for each new procurement request which will result in a classified contract. The DD 254 shall not be classified.

3. Contract Security Classification Specification (DD 254)

a. Each procurement request or other document which requires access to classified information for contractual performance must be accompanied by a DD 254. The responsibility for preparation of the DD 254 rests with the program office having technical cognizance over the procurement. DD 254s are legal contractual documents and will be signed by the

[102 2 8 000]

contracting officer's technical representative and either OPNAV (DNS-34) , (DNS-34B) or (DNS-34D), who are designated as Contracting Officer's Representative (COR) representatives by billets (occupation code 0080) as delineated in reference (b).

b. Cognizant technical offices will prepare a draft DD 254 following the instructions provided in exhibits 15A and 15B, forward the drafted DD 254, the statement of work, and classification guides to OPNAV (DNS-34) for review prior to finalizing.

c. The cognizance technical office will also review the DD 254 biennially, as well as whenever classification guidance changes. The results of reviews will be furnished to OPNAV (DNS-34). Biennial review and/or final DD 254 will not be required when the contract provides access only to classified information/material or the contract is a service type contract. OPNAV (DNS-34) will notify cognizance technical offices when contracts are due for review.

d. When final delivery of the end item has been completed and retention of classified material is requested, a final DD 254 will be prepared. OPNAV (DNS-34D) will coordinate requests for retention for classified material, verify "need-to-know" and any other security or classification matter. Replies to the requestor will be prepared by OPNAV (DNS-34D) and a copy will be sent to the cognizance technical office.

4. Classified Visits to OPNAV Security Serviced Activities by Contractor Personnel

a. Refer to chapter 14 of this instruction for policy regarding classified visit by contractor personnel.

b. Access to intelligence information will not be authorized unless the following information is included in the visit request:

(1) The contractor's certification that access to classified intelligence is required for contract performance and the contract is a classified contract;

(2) Sufficient information to allow evaluation and applicability of the contractor's performance requirements;

MAR 23 2009

(3) Certification to release classified intelligence to contractors without permission of the originator and/or sanitation of the material; and

(4) Specific program or project involved with the level of information to be released; certification from the UA that the visitor has been authorized access to such information and the identity of the office or UA activity granting such authorization.

c. If access to classified information requiring a special access authorization (i.e., NATO, military space project or other special or limited access programs), the request will, in addition to the other required information:

(1) Specify the program or project;

(2) Specify the level of information to be released;

(3) Certify from the UA that the visitor has been authorized access to such information; and

(4) Provide identity of the office or UA activity granting such authorization.

d. If contract performance is to be in whole or part on-site (within office spaces), obtain approval of OPNAV (DNS-34) to ensure that all security requirements are addressed. Contractor employees are not attached to the command, therefore, do not come under administrative control of the command. Security issues pertaining to on-site contract performance must be included in the DD 254 or appended as a supplemental security requirements. Refer to item 13, exhibit 15A, and exhibit 15B.

5. Dissemination of Classified Material to DoD Contractors

a. Classified material will only be disseminated to contractor personnel as outlined in this chapter and chapter 9 of this instruction.

b. Policy regarding the hand carrying of classified material by contractor personnel out of OPNAV's spaces is contained in chapter 6 of this instruction.

c. All classified material to be forwarded to contractors' facilities will be processed through the SECNAV/AAUSN mail room or OPNAV (DNS-34C), as applicable.

MAR 23 2009

d. Classified material must be sent with a letter of transmittal and OPNAV 5216/4 Outgoing Mail Record. The letter of transmittal will contain the contract number under which the classified material is being released. In addition, the releasing office will verify the facility clearance, safeguarding capability and classified mailing address as outlined in chapter 10 of this instruction.

e. Access to classified information by a contractor is normally justified when:

(1) A bona fide contractual relationship exists between the contracting organization and the UA; or

(2) Access is required in connection with pre-contract negotiations; and

(3) The organization has a current facility clearance commensurate with the classification of the information to which access is requested; and

(4) The person(s) for whom the access authorization is intended has a personnel security clearance commensurate with the information to which access is requested; and

(5) The person(s) for whom access is requested has a valid "need-to-know."

6. Procedures for Issuance of DoD Building Passes to Contractor Personnel. The policies and procedures regarding the issuance of DoD building passes to contractor personnel are contained in chapter 3 of this instruction.

7. Consultant Clearances

a. The information contained in this section refers to those consultants hired under the provisions of the OPM but are not paid. Consultant clearance will not be processed unless the consultant is approved and processed via the civilian personnel office.

b. In all cases, personnel security clearances/facility security clearances/classified storage capability for self-employed consultants shall be processed in accordance with the provisions in reference (k) and the following:

MAR 23 2003

(1) TYPE A - The consultant does not possess classified material, except at the UA activity or while on authorized visit to another Government agency/cleared contractor facility. The consultant, for security administrative purposes only, shall be considered as an employee of the UA.

(2) TYPE B - The consultant possesses classified material at his/her place of business or residence and has full responsibility for the security clearance and classified storage. Type B consultants will be considered as prime contractors to the UA. The execution of a DD 254 is required. Refer to exhibit 15A for instructions in the preparation and use of DD 254.

(3) TYPE C - The consultant possesses classified material at his/her regular employer's cleared facility, and the consultant and his/her employer having agreed as to their respective responsibilities for security of the classified material. A copy of this agreement must be on file with OPNAV (DNS-34).

c. Type A, B and C consultant clearances will be processed by OPNAV (DNS-34). Requests shall be submitted to OPNAV (DNS-34) from S/HHRO as all other civilians hired. Applicable forms required for processing type A, B, and C consultant clearances will be disseminated by OPNAV (DNS-34B) upon approval of request.

d. Access to classified information will not be granted to consultants until the Defense Industrial Security Clearance Office (DISCO) has issued a Letter of Consent (DISCO Form 560) to OPNAV (DNS-34). Although a prospective consultant may have a current valid clearance with a DoD contractor, it is not for use as an OPNAV security serviced activity consultant. A concurrent clearance must be obtained by OPNAV (DNS-34) from DISCO.

e. Security coordinators are responsible for ensuring that consultants check in and out with OPNAV (DNS-34). Check-out procedures will consist of return of building passes and written verification from the cognizance security coordinator that the consultant has been debriefed and all classified material has been returned to the employing office. OPNAV (DNS-34) will execute a DISCO Form 562 Personnel Security Clearance Change Notification or execute a final DD 254 to administratively terminate the individual's clearance.

MAR 23 2009

EXHIBIT 15A

S-A-M-P-L-E

PROCEDURES AND GUIDELINES ON PREPARATION OF DD 254

1. The following security questions will be considered early in the acquisition cycle: (1) Will access to classified information be required? (2) Will access be required during the pre-award phase, or will it only be required for actual performance of the contract? (3) Are all the prospective contractors cleared to the appropriate levels? (4) Are contractors equipped to properly safeguard the classified information? The answers to these questions and the timeliness of command action will have a significant impact on acquisitions and the National Industrial Security Programs (NISP). Proper lead time in the acquisition cycle must be provided to accomplish the required security actions. In many instances, advanced planning can ensure that the bid package will not require access to classified information, and prevent processing an entire bidders list for facility security clearances. When access is required in the pre-award phase, an interim facility security clearance may be the solution. If access is not a factor in the pre-award phase, but will be required for contract performance, only the successful bidder will be processed for a facility clearance. Processing unnecessary prospective contractors for facility clearances is very time consuming and costly. Determine the security requirements for the proposed contract as follows:

a. Access to classified information. Requires a "classified contract" under the NISP. Certain security clauses must be incorporated in the solicitation and in the contract, and certain security clearances will be required.

b. No Access required in the pre-award phase. Prospective contractors do not have to possess facility security clearances to bid on the solicitation. Only the successful bidder must have an appropriate facility security clearance and safeguarding capability.

c. Access required during the pre-award phase. All prospective contractors must possess the appropriate facility clearance and safeguarding capability during this phase.

MAR 23 2009

2. After decision on the security requirements, determine the current clearance status of all prospective contractors:

a. All prospective contractors have appropriate clearance. No further clearance action is needed.

b. Some prospective contractors do not have appropriate clearances. All prospective contractors must have an appropriate clearance prior to release of the information. A request must be submitted to the Cognizant Security Office (CSO) furnishing the appropriate information needed to process the clearance.

3. The next step is to determine what security classification guidance the contractor will need to perform on the contract. A DD 254 is required for each classified contract and must be incorporated in the solicitation and in the contract. Even if pre-award access is not required, the DD 254 should be incorporated in the solicitation to provide the contractor with information needed during contract performance. If pre-award access is not required, add the following notation in item 13, "Security Guidance" of the DD 254. "Pre-award access is not required. This DD 254 reflects the security requirements for the contract when awarded."

4. The DD 254, issued with the solicitation Request For Quote (RFQ), Request For Proposal (RFP), or Invitation For Bid (IFB), is always an "original." When the contract is awarded and the contract number is assigned, another "original" DD 254 is issued reflecting the contract number and date of issuance. The following correspond to the numbered items of DD 254: (see paragraph 6 of this instruction for DD 254 acquisition):

Item #1: Insert the highest level of facility clearance (includes personnel) required for access to classified information in the performance of the contract. Use only the words "Top Secret," "Secret," or "Confidential." Special caveats such as RD, FRD, COMSEC, SCI, will not be indicated in this block. The facility security clearance of the contractor shown in item 1b must be at least as high as the classification indicated in item 1a. If the contractor will not need to possess or store classified at the facility, enter "not applicable" or "none" (if this is the case, item 1a must be marked "Yes.")

MAR 28 2003

Item #2: For actual contract when awarded, place an "X" in item 2a, or for an RFP, REQ, or IFB place an "X" in item 2C.

Item #2b: For sub contractor, DD 254 is completed by the prime contractor. The prime contract number must be entered in item 2a.

Item #2c: For RFP, RFQ, IFB or other solicitation, regardless of whether or not the bid package will contain classified information, must also include date by which bids are due.

Item #3a: Complete when the actual contract or subcontract has been awarded.

Item #3b: When there is a change in classification guidance or sequential revisions, enter the date of revision with date of original in item 3a. Information is completed by the prime contractor for subcontractor.

Item #3c: Completed upon extension of retention authority (see reference (k), chapter 5, section 7 for more on disposition and retention).

Item #4: A follow-on contract is a contract that is granted to the same contractor or subcontractor for the same item or services as a preceding contract. When this condition exists, mark "Yes" and enter the preceding contract number in the space provided. This item authorizes the contractor or subcontractor to transfer material received or generated under the preceding contract to the new contract. The material transferred should be reflected in item 13.

Item #5: If this is a final DD 254, mark "Yes" and enter the date of the contractor's request for retention and the authorized period of retention in the space provided. If this is not for a final, mark "No."

Item #6: Used to provide Government guidance to a prime contractor. Enter information as follows:

Item #6a: Name and address information.

Item #6b: The contracting office (formerly DISCO).

Item #6c: Identifies the appropriate DSS field office responsible for inspection of the contractor facility. (See

MAR 28 2000

appendix A of reference (k) or contact local DSS office for more details.) Verify the cleared classified mailing addresses for contractors.

Item #7: If the DD 254 is for a subcontractor, enter information as above (item 6) for the subcontractor. Items 6a, 6b, and 6c may be left blank. Verify the cleared classified mailing address for contractors.

Item #8: If work is to be performed at a location other than specified in item 6a (or item 7a, as appropriate), enter actual work location. If multiple, use block 13 or addendum sheet. Explain performance on Government facility in item 13.

Item #9: Enter a description of the procurement. This may be material, studies, services, etc. The statement should be short, concise, and unclassified.

Item #10: Mark all items "Yes" or "No" as appropriate to the requirement of the contract. This action requires coordination with the appropriate program and other security offices to ensure the proper type of access is imposed on the contractor or subcontractor.

Item #10a: COMSEC information includes accountable or non-accountable COMSEC or cryptographic items. If accountable COMSEC is involved, the contractor must have a COMSEC account and item 11h must be marked "Yes." Prior approval from the Government control agent is required prior to prime contractor negotiating or granting COMSEC to subcontractor.

Item #10b: Must be marked "Yes" if item 10c is marked "Yes."

Item #10c: Government Contracting Authority (GCA) approval is required prior to granting CNWDI access to a subcontractor.

Item #10d: Marked "Yes" if access to FRD is required.

Item #10e: The Government representatives are responsible for ensuring any additional requirements are incorporated as addendum to DD 254 and provided to the contractor. If SCI access is required, mark "Yes." Items 14 and 15 must be marked "Yes." Item 1b must be marked "Top Secret." Mark item 10e(2) "Yes" if access to non-SCI is required. Item 14 must be marked "Yes," and item 15 must be marked "No." If access to SCI and non-SCI is requires, mark item 10e(1) and item 10e(2) "Yes."

MAR 23 2009

Item 14 must be marked "Yes," and item 15 is marked as appropriate. Prior approval from the Government is required before a subcontractor involving access to intelligence information can be issued.

Item #10f: SAPs impose requirements on the contractor that exceed reference (k). When SAP information is involved, the program manager and COR are responsible for providing the contractor with the additional security requirements needed to ensure adequate protection of the information. The additional requirements would be included in the contract document itself, item 13 or both, or as an addendum to the DD 254. If item 10f is "Yes," mark item 14 "Yes" and complete item 15 as appropriate because some SAPs qualify as carve-outs. If an SAP subcontract is awarded, it is the prime contractor's responsibility to incorporate the additional security requirements in the subcontract. Authority for access must be obtained from the program managers and COR.

Item #10g: Mark "Yes" if the contract requires access to information or documents belonging to NATO.

Item #10h: This item includes any foreign government information except NATO. Mark "Yes" if applicable.

Item #10i: This is no longer a valid program and there should not be any new documents or contracts reflecting this caveat. Until the DD 254 is revised, this block should be marked "No".

Item #10j: This item may be applicable on some classified contracts. When this item is marked "Yes," the GCA is responsible for providing the contractor with the safeguards necessary for the protection of the information. Reference (k) does not provide guidance concerning FOUO, so the GCA must provide guidance on protection procedures in item or addendum to DD 254.

Item #10k: Is used for any other information not included in items 10a through 10j. Specify the type of information and include any additional remarks in item 13.

Item #11a: Is used for access to classified information only at other contractor/Government facilities. Note the word "only." If the "Yes" box is marked for this item, item 11b must be marked "No," and the remaining items marked as required. The contractor will not be required to have any safeguarding

MAR 23 2009

capability at his/her facility if this item is marked "Yes." The following notation, "Contract performance is restricted to (name of contractor or Government activity) and location," shall be added in item 13. Using Government activity will furnish complete classification guidance for the service to be performed. .

Item #11b: Used for receipt of classified documents or other material for reference only (no generation). Note the word "only." If the "Yes" box is marked for this item, items 11a, 11c thru 11e must be marked "No" and the remaining items marked as required. The contractor will be required to have safeguarding capability at his facility.

Item #11c: Receipt and generation of classified documents or other material. If the "Yes" box is marked, appropriate security guidance will be included in item 13, or attached to DD 254, or forwarded under separate cover, or included in the contract documents itself. If marked "No," the remaining items 11a, 11b and 11e must be marked "No" and the contractor must have safeguarding capability at his facility.

Item #11d: Fabrication/Modification/Storage of classified hardware. If applicable, include as much information as possible (additional information can be added in item 13) to indicate if restricted or closed areas will be required. How much hardware and storage are involved? How large? When does the hardware become classified?

Item #11e: Graphic Arts Services Only. Note the word "only." If the "Yes" box is marked for this item, items 11a thru 11d must be marked "No," and the remaining items marked as required. This type of contract would not require any specific classification guidance because the markings on the documents provided would be sufficient guidance for the contractor. The contractor will be required to have facility safeguarding capability. The following notation will be added to item 13:

Graphic Arts Services. "Reproduction services only. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract."

Engineering Services. "Contract is for engineering services. Classification markings on the material to be

MAR 23 2009

furnished will provide the classification guidance necessary for the performance of this contract."

Equipment Maintenance Services. "Contract is for equipment maintenance services on equipment which processes classified information. Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information can not be precluded by escorting personnel. Any classification guidance needed will be provided by the contractor."

Guard Services. "Contract is for guard services. Cleared personnel are required by reference (k) to provide supplemental protection."

Item #11f: If "Yes," indicate in item 13 the U.S. activity where the overseas performance will occur. Also list the city and country. Item 14 may be marked "Yes" and completed as appropriate depending upon the programs involved. Item 15 should also be completed as appropriate.

a. For DoD contractors performing on overseas contracts, provide a copy of the DD 254 to the appropriate DSS Office of Industrial Security, International. (See reference (k), appendix A, or contact DSS.)

b. See reference (k), paragraph 10-204, for suggested "Security Clauses for International Contracts" for classified contracts involving foreign contractors.

Item #11g: Mark "Yes" if the contractor is to be authorized use of Defense Technical Information Center (DTIC) services. DD 1540 Registration For Scientific and Technical Information Services and DD 2345 Military Critical Technical Data Agreement must be completed for registration with DTIC.

a. The sponsoring GCA submits the DD 1540 to DTIC on behalf of the contractor. For subcontractors, the prime contractor submits the DD 1540 with the Government verifying "need-to-know."

b. The contractor may also submit DD 2345 (after registration with DTIC) to the Defense Logistics Services Center for access to unclassified, militarily critical technical data

MAR 23 2003

from other DoD sources. The Government authority must certify the "need-to-know" to DTIC.

c. See reference (k) chapter 11, section 2 for more information.

Item #11h: Require a COMSEC account. Mark this item "Yes" if accountable COMSEC information must be accessed in the performance of the contract. If not accountable COMSEC information is involved, mark this item "No."

Item #11i: Have TEMPEST requirements. Mark "Yes" if the contractor is required to impose TEMPEST countermeasures on information processing equipment after vulnerability assessments are completed. TEMPEST requirements are additional to the requirements of reference (k). Thus, prime contractors may not impose TEMPEST requirements on their subcontractors without Government authorities approval.

a. If marked "Yes," item 14 must also be marked "Yes" and pertinent contract clauses identified or added to item 13.

b. If requested by the Government authorities, TEMPEST countermeasure assessment requests may be included as an attachment to the DD 254.

Item #11j: Have Operations Security (OPSEC) requirements. Mark "Yes" if the contractor must impose certain countermeasures directed to protect intelligence indicators. OPSEC requirements are additional to the requirements of reference (k). Thus, contractors may not impose OPSEC requirements on their subcontractors unless the Government authorities approve the OPSEC requirements. If marked "Yes," item 14 must also be marked "Yes" and pertinent contract clauses identified or added to item 13.

Item #11k: Be authorized to use the DCS. A "Yes" in this block authorizes the contractor to use the services of DCS. The Government authorities must obtain written approval from the Commander, Attn: Operations Division, Fort George G. Meade, MD. 20755-5370. Only certain classified information qualifies for shipment by DCS. The Government authorities are responsible for complying with DCS policy and procedures. Prior approval of Government authorities is required before a prime contractor can authorize a subcontractor to use the services of DCS.

MAR 23 2009

Item #111: Other (specify). Use this item to add any additional performance requirements not covered above. Item 13 should be appropriately annotated to provide any necessary remarks.

Item #12: Public Release

a. The contractor is responsible for obtaining the approval of the contracting activity prior to release of any information received or generated under the contract, except for certain types of information authorized by reference (k).

b. Government authorities should complete this item as required by internal agency directives to direct the prime contractor to the appropriate office of the Government authorities that have public release authority. Prime contractors should refer their subcontractors to the Government authorities' office that was referenced in the prime contract DD 254.

Item #13: Security Guidance

a. Use this block to expand or explain information referenced in other sections of the DD 254. When completing item 13, consider the following questions:

(1) What classified information will the contractor need in the performance of this contract?

(2) Is there an existing security classification guide for the program?

(3) If subcontracting, is the guidance in the prime contract DD 254 adequate? Does the entire prime contract DD 254 apply to the subcontract or do you only need to provide applicable portions?

(4) Will classified source documents be used? If so, do they contain all the guidance the contractor needs?

(5) What will the contractor's actual performance be? (e.g., Research and Development (R&D), test, production, study, etc.)?

MAR 23 2009

(6) What unique characteristics are involved that need protection? Are there design features which require protection? Is there technical information which will require protection?

(7) What breakthroughs would be significant if achieved in an R&D effort?

(8) Are there performance limitations that require protection?

(9) Will classified hardware be furnished to or generated by the contractor?

(10) What information makes the hardware classified?

(11) Will hardware being generated require classification? At what stage in its production does it become classified?

b. These are some of the questions that should be asked when preparing guidance for a contractor. Put yourself in their place; do you understand the guidance? Will they be sure to:

(1) Identify the specific information to be classified;

(2) Provide appropriate downgrading or declassification instructions; and

(3) Provide any special instructions, explanations, comments or statements necessary to clarify other items identified in the DD 254.

c. A factor to consider when completing item 13 is that each contract is unique in its performance requirements, therefore, a standardized format may not necessarily be the best for every DD 254.

d. Give reasons for classification.

e. Write the guidance in plain English so it can be easily understood. Use additional pages to expand or explain guidance. Be as specific as possible and include only that information that pertains to the contract for which it is issued. Avoid references to internal directives and instructions. If such documents provide guidance applicable to the contract, extract the pertinent portions and provide them as attachments. All

MAR 23 2003

documents cited in item 13 should be provided to the contractor either as attachments or forwarded under separate cover. Do not extract the requirements of reference (k) or its supplements and include them in a DD 254. Reference (k) provides safeguarding requirements and procedures for classified information, not classification guidance. Encourage participation by the contractor in the preparation of the guidance and submission of comments and/or recommendations for changes in the guidance that has been provided.

Item #14: Complete this item whenever security requirements are imposed on a contractor in addition to the requirements of reference (k) or its supplements. Keep in mind that additional requirements translate into additional cost so it is essential that you coordinate with program and other security offices to ensure you are imposing appropriate requirements on the contractor.

a. A "Yes" in this item requires the Government authority or prime contractor to incorporate the additional requirements in the contract itself to negotiation or reference in item 13.

b. Costs incurred due to additional security requirements are subject to negotiation between the contractor and the Government.

c. Prior approval by the Government is required before a prime contractor can impose additional security requirements on a subcontractor.

d. A copy of the DD 254 containing the additional security requirements should be provided to the contract security officer.

Item #15: Mark "Yes" if the contract security officer is relieved, in whole or in part, of the responsibility to conduct security reviews and provide security oversight to the contractor. Information should be provided regarding the specific areas from which the contract security officer is excluded and the agency that will assume the responsibility. The contractor security officer is relieved of the responsibility to inspections as follows:

a. SCI material. When access to SCI is required (item 10.e (1)), the following statement must be added: "appropriate agency/military department senior intelligence officer has

MAR 23 2009

exclusive security responsibility for SCI classified material released or developed under this contract and held within the contractor's SCIF."

b. SAPs. Where the program security office has "carved out" the contract security officer from inspection responsibility. Not all SAPs are "carve outs," and in some instances, the program security office will allow the contract security officer to retain inspection responsibility.

Item #16: The certifying official for OPNAV DD 254s will be career security specialist (occupation code 0080) as delineated in reference (b). Coordinate with OPNAV (DNS-34) for the signing the DD 254. Individual signing the DD 254 will ensure it has been adequately staffed among the appropriate contracting, program and security personnel.

Item #17: Distribute copies of the DD 254, as appropriate, and indicate the distribution in the respective blocks. Additional copies can be distributed internally to visit control offices, contracts offices, departmental personnel, etc.

MAR 23 2009

EXHIBIT 15B

S-A-M-P-L-E

GUIDELINES FOR ON-SITE CONTRACT PERFORMANCE

1. Before initiating procurement actions for contractor performance, in whole or in part on-site (within OPNAV spaces), approval must be obtained from OPNAV (DNS-34) to ensure that all security requirements are addressed. Provide OPNAV (DNS-34) with copies of the "Statement of Work" and drafted DD 254. Contractor employees are not attached to the command, therefore, do not come under administrative control or authority of the command. However, by including applicable requirements in the DD 254, we can commit the Navy and hold the contractor facility responsible for items which are identified. Security requirements may also increase the contract costs, so do not unnecessarily include security items that need not be performed by the contractor. Having contractor employees on access lists and acting as custodians for classified material/spaces is not encouraged and must only be requested when contract performance cannot be achieved by any other means.

2. Once it has been determined that contract performance is required on-site and the contractor(s) will be responsible for security aspects, the requirement will be included in the DD 254 in item 13 to include applicable additional security regulations, procedures, instructions, etc. The DD 254 is the only way to enforce the security requirements. A contractor employee cannot be responsible for securing a classified container unless it has been put in writing and applicable security guidance regarding such actions has been provided. IA tasks are the most common duties performed by contractor employees on-site. In these cases, the command IA security program must apply to the contractor and be addressed in the DD 254.

3. In addition to including the on-site performance requirement in the DD 254, the following items must be considered and executed as applicable on a case-by-case basis:

a. Provide the contractor written instructions specifying:

(1) Those security actions, if any, which will be performed for the contractor by the installation, such as

MAR 23 2000

providing storage facilities, guard service, mail and freight services, visit control, and;

(2) Those security actions, if any, for which joint action may be required such as the packaging and addressing of classified transmittals, and control of visitors.

b. Ensure that the contractor has prepared a Standard Practice Procedure (SPP) covering the contractor's activities on the installation, if appropriate.

c. Ensure that the contractor observes required security controls through periodic inspections in accordance with security regulation and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

d. Ensure that prompt remedial action is taken when security conditions are deficient in the contractor's operations.

e. Ensure that the DoD Security Education Program is implemented by the contractor and, as required, conduct defensive security briefings required by reference (k) for safeguarding classified information.

f. Conduct investigations of contractor security violations, including loss, compromise, or suspected compromise of classified information.

g. Conduct the briefing and debriefing of the Facility Security Officer (FSO), the COMSEC custodian, and alternate COMSEC custodian when there is a COMSEC account or there is a requirement to establish a COMSEC account. Brief and debrief only the FSO if there is no COMSEC account.

h. Furnish to the contractor guidance on the application of security requirements to the contractor's operations.

i. Forward requests from the contractor for interpretations of reference (k) to the CSO.

j. Request interim personnel clearance levels from DISCO for contractor personnel, when required, to prevent crucial delay in the performance of the contract.

MAY 28 2000

k. Ensure that the contractor reports promptly any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information. In addition, the CSO of the visiting contractor's facility shall be advised concerning the incident.

4. The SPP will include in sufficient detail to place into effect all security controls required in addition to reference (k) which are applicable to the contract on-site operation.

5. Normally, all defensive security briefings will be provided to the contractor (e.g., orientation, refresher, counterespionage, etc.) by their contractor facility. However, when required for unique training applicable to only the contractor employee(s) performing contract work on-site, briefings will be provided by the installation. In any case, if the on-site contractor employee requires a foreign travel briefing, the installation must be notified by the contractor facility for record purposes even though the contractor facility will be providing the briefing to the employee.

6. The purpose of these guidelines, when required, is to have a contractor employee responsible to applicable security regulations, policies, instructions, when they must perform a security function on-site in the same manner in which an employee would.

MAR 23 2009

CHAPTER 16
COMPROMISE AND OTHER SECURITY VIOLATIONS

1. General

a. It is the duty of each individual assigned to a sensitive billet to comply with the provisions of chapter 12 of reference (b), as related to the reporting of loss, possible loss, or subjection to compromise of classified information. Reports of loss, possible loss, compromise, possible compromise and violations of security regulations will be reported to OPNAV (DNS-34) via security coordinators. In case of computer spills, the supervisor, security coordinator, security manager, Customer Technical Representatives (CTR), or alternate, and the IA manager must be advised soonest in accordance with established Navy Marine Corp Intranet (NMCI) procedures.

b. There are two types of security violations: one which results in compromise or a possible compromise of classified information; the other results in security regulations being violated but no actual compromise occurs.

c. Compromise is the disclosure of classified information to a person who is not authorized access. The unauthorized disclosure may have occurred knowingly, willfully or through negligence. A compromise is confirmed when conclusive evidence exists that classified information has been disclosed to an unauthorized person. A possible compromise is when some evidence exists that classified information may have been subjected to unauthorized disclosure. Both allegations are confirmed for OPNAV security serviced activities through official Preliminary Inquiries (PIs) as outlined in paragraph 2 of chapter 16 of this instruction (report symbol OPNAV 5510.6B applies per reference (b), appendix C). A JAG manual investigation (report symbol OPNAV 5510.6C applies per reference (b), appendix C) is a potential recommendation resulting from a PI to provide a more detailed investigation and recommend disciplinary action or additional corrective action. NCIS is available for investigative assistance.

d. Compromise presents the greater threat to national security, but other security violations must also be treated seriously because they demonstrate that a weakness exists in a command's security program. For this reason, security violations of either type must be reported, vigorously investigated and corrected rather than covered up. Incidents of an individual's failure to comply with the policies and

MAR 23 2003

procedures for safeguarding classified information will be evaluated to determine eligibility to hold a security clearance.

e. Per reference (b), classified information is considered compromised if it has been handled through a foreign postal service, its shipment container has been damaged to expose the content, or it has been transmitted over unprotected communications circuits.

f. Electronic Spillage (ES) occurs when data is on a computer system that has not been accredited with appropriate control measures to provide adequate protection at the required classification. All hands will pay strict adherence to IA and NMCI guidance for reporting, scrubbing and recovery of ES in accordance with requirements outlined in chapter 18 of this instruction.

2. Security Violations

a. When OPNAV (DNS-34) has determined that there has been a security violation, OPNAV 5511/5 Security Violation Report will be sent from OPNAV (DNS-34) to the OPNAV security serviced activities concerned on behalf of CNO (DNS). Command authorities shall appoint, in writing, a command official, other than subordinates to potential culprits or anyone involved in the incident, to conduct a PI. A PI will be conducted by the appropriate security coordinator or other designated official. To avoid a conflict of interest, no individual involved or suspected of involvement with a security violation will be permitted to act as an inquiry official, nor will inquiry report results be reported via any individual involved or suspected with a security violation.

b. PIs will be completed within 3 days from receipt of the request, signed by OPNAV (DNS-34), and must:

(1) Strictly adhere to the requirements of reference (b), chapter 12 (exhibit 12A) and will accurately identify the information lost, compromised or subjected to possible compromise, to include:

- (a) Classification of the material;
- (b) Identification/serial numbers;
- (c) Date;

MAR 23 2003

(d) Originator's contact information and guidance;

(e) OCAs;

(f) Subject;

(g) Downgrading/declassification;

(h) Number of pages/or units of information;

(i) Command's point of contact information; and

(j) Unit Identification Code (UIC) of custodial command.

(2) Determine the circumstances surrounding the incident and identify any requirements for additional command action.

(3) Identify all witnesses to the violation and informally interview them to determine the extent of the violation.

(4) Identify the individual responsible, if possible.

(5) Make an attempt to discover the weakness in security procedures that allowed the compromise or subjection to compromise to occur.

(6) Evaluate the information compromised or subjected to compromise to determine the extent of potential damage to national security, and the action necessary to minimize the effects of the damage.

(7) Include a statement that the NCIS field office, Naval Investigative Service Resident Agency (NISRA), Washington Navy Yard, telephone (202) 433-3858, has been advised and accepted or declined investigation responsibility. Can also contact the OPNAV assigned onboard NCIS support officer at (703) 692-8988.

(8) Establish either:

(a) That an unauthorized disclosure of classified material did not occur (see subparagraph 2c below), or the compromise may have occurred but under circumstances presenting a minimal risk to national security (see subparagraph 2d below); or

MAR 28 2000

(b) That compromise is confirmed and that the probability of damage to the national security cannot be discounted (see subparagraph 2e below).

c. If it is determined that a compromise or possible compromise in fact did not occur, the inquiry will be terminated and report of inquiry will be sent via the OPNAV security serviced activity and OPNAV (DNS-34) to Deputy Director Navy Staff (DDNS). No further reporting is required.

d. If a determination of possible compromise:

(1) Minimal risk is made;

(2) No significant command security weakness is found;

and

(3) When formal disciplinary action is not appropriate, the inquiry will be sent back to OPNAV (DNS-34). If OPNAV (DNS-34) agrees that conditions have been met, notification of the originator of the material involved is required. The OPNAV security serviced activity will notify the DoD originators that no further action will be taken with copy to CNO (N09N) and NCIS, Washington, DC. CNO (N09N) is the designated authority for notifications of compromises to originators of the material that are outside of DoD.

(4) If OPNAV (DNS-34) does not agree that conditions have been met, concurrence will be sought from DDNS and a JAG manual investigation will be directed. A copy of the investigation results will be sent via CNO (DNS) to CNO (N09N).

e. If the OPNAV security serviced activity conducting the inquiry determines that:

(1) Compromise is confirmed; and

(2) Probability of damage to national security cannot be discounted; or

(3) Significant activity weakness is revealed; or

(4) Punitive action is appropriate, then a JAG manual investigation will be initiated.

MAR 23 2009

(5) The PI will be sent directly to the originator of the material involved, if in DoD, advising that further investigation is being conducted with information copies to DDNS, CNO (N09N) and NCIS.

(6) If the originator of the material is outside of the DoD, send the report to CNO (N09N) who will notify the originator.

f. PIs will be forwarded to OPNAV (DNS-34) (on behalf of DDNS) not later than 3 days after the violation report is received from OPNAV (DNS-34). If more time is required to complete the report, notify OPNAV (DNS-34) in writing of the reason for delay and the expected date of completion.

g. Reporting losses or compromises of special types of classified information and equipment:

(1) Report losses or compromises of SCI to OPNAV (N21).

(2) Report losses or compromises of classified computer system information, terminal or equipment to CTR, NMCI and the OPNAV Security Manager (OPNAV (DNS-34)) who will notify OPTI, OPNAV (DNS-4), OPNAV (N09N2) and Deputy Chief of Naval Operations, Communications Networks (CNO (N6)) when warranted.

(3) Report losses or compromises of NATO classified information to OPNAV (DNS-34C) who will notify OPNAV (DNS-34) and the Central United States Registry and OPNAV (N09N2) when warranted.

(4) Report losses or compromise of DoD SAPs to Head, Special Programs Branch (OPNAV (N89)).

(5) Report losses or compromises of NC2-ESI to OPNAV (N5JA) who will notify the Joint Chiefs of Staff (JCS), OPNAV (DNS-34) and OPNAV (N09N2).

(6) Report losses or compromises of RD (including CNWDI and FRD) to OPNAV (DNS-34) who will notify OPNAV (N09N2) for further reporting to DOE with copy to NCIS.

(7) Report losses or compromises of COMSEC to EKMS manager, NCMS Washington, DC, for further reporting to DDNS, OPNAV (N09N2), NCIS and NSA. Provide courtesy copy to OPNAV (DNS-34).

MAR 23 2009

(8) Any incident indicating a deliberate compromise of classified information or possible indications of foreign government or intelligence involvement in collection against the United States will be reported to NCIS.

(9) DoD regulations require that FOUO, personal and Privacy Act data be protected from unauthorized disclosure. Unauthorized disclosure could result in civil and criminal sanction against responsible individuals. Personnel and military departments will be notified when FOUO, personnel and privacy data are disclosed or compromised.

h. The cognizance OCA must be notified when classified information under their programs have been compromised in order to ensure appropriate damage assessment and security and classification reviews are conducted. Final authority to declassify or maintain appropriate classified level of the compromised information remains with the OCA.

3. Administrative Sanctions, Civil Remedies, and Punitive Actions

a. Civilian employees are subject to administrative sanctions, civil remedies, and criminal penalties if they knowingly, willfully or negligently disclose classified information to an unauthorized person or knowingly, willfully, or negligently violate provisions of this instruction and the provisions of reference (b) for classification and protection of classified information. Sanctions include, but are not limited to: a warning notice, reprimand, and suspension without pay, forfeiture of pay, removal and discharge. See Civilian Human Resources Manual, subchapter 752, of 6 January 2004 for a description of adverse personnel actions and their application.

b. Military personnel are subject to punitive action, either in civil courts or under UCMJ, as well as administrative sanctions, if they disclose classified information to an unauthorized person or violate provisions of this instruction and the provisions of reference (b) for classification and protection of classified information. When a court-martial is recommended as a punitive action for compromise or other security violation, as with court-martial for other reasons, notify the local JAG office immediately so they can draw up the charge and specification.

MAR 23 2003

c. Disciplinary action is used primarily to make it clear to the offender, and other personnel, that security procedures must be followed without deviation. Action taken for involvement in security violations should suit the offense and be applied regardless of rank, rate or grade. Within OPNAV security serviced activities, the minimum corrective action for security violations is the presentation of a non-punitive letter of caution to the individual, military or civilian, responsible.

d. Security regulations require that performance rating system of all DON personnel, whose duties significantly involve creation, handling, or management of classified information, include a critical security element on which to be evaluated.

4. Review of Violation Reports. DDNS will be briefed on all completed investigation reports to ensure that the findings of the preliminary investigation are complete and appropriate corrective action has been taken to preclude reoccurrences. Where insufficient or inappropriate action appears to have been taken, DDNS will recommend further investigation.

MAR 23 2009

CHAPTER 17
FORCE PROTECTION MEASURES AND PLANNING

1. Introduction. Terrorism is the unlawful use of or threatened use of force or violence by a person or organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reason. Acts of terrorism directed at naval personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage through adverse publicity.

2. Responsibilities

a. PFFPA is responsible for protection of the Pentagon Reservation, its occupants, and Government and private property. OPNAV (DNS-34) interfaces with PFFPA and, in consonance with regulations and guidelines, administers security enforcement procedures within OPNAV security serviced activities through the security coordinators.

b. Physical protection for the OPNAV security serviced activities spaces located within the Pentagon and other swing spaces resides with PFFPA. Physical security, including safeguarding, storage and related policy within those spaces, is managed by OPNAV (DNS-34).

c. Each OPNAV security serviced activity exercises command responsibilities and security enforcement authority within the spaces of their respective organization.

3. Force Protection Conditions (FPCONs)

a. JCS has established a series of threat conditions and corresponding measures to facilitate inter-service coordination and support U.S. military anti-terror activities. In the Washington, DC, area, these conditions would normally be set and force protection measures implemented by the Commandant of the Military District of Washington, based on threat intelligence. Security FPCONs on the Pentagon Reservation will be announced by PFFPA with emergency procedures being directed under the Pentagon Evacuation Plan. OPNAV security serviced activities located outside the Pentagon will fall under the security plan established by their building manager and executed through PFFPA. FPCONs standardize the military services' identification of

MAR 23 2009

terrorist threats against U.S. personnel and facilities; also referred to as FPCONS. There are four FPCONS levels as follows:

(1) ALPHA. This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCON resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

(2) BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

(3) CHARLIE. This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

(4) DELTA. This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this FPCON is declared as a localized condition.

b. Homeland Security Threat Levels. The below color-diagram provides the corresponding Homeland Security threat levels that are used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the command, community and the nation. The Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries based on specific threat information.

MAR 23 2003



c. OPNAV (DNS-34) will engage with PFPA as situation dictates and provide coordination of measures across OPNAV security serviced activities for specific checks, evacuation plans, spot checks and personal restrictions as may be required.

d. Bomb Threat. PFPA has the responsibility for investigating bomb threats within the Pentagon. They will not be able to perform this task successfully unless the person receiving the call takes proper action and gets as much information as possible. To ensure that OPNAV security serviced activities personnel answering telephones take proper action while under the stress of a bomb threat, a Bomb Threat Record, identified at chapter 19, subparagraph 2g, of this instruction will be used. Bomb threats in the Pentagon should be reported to PFPA at (703) 697-5555.

ENC 28 200

CHAPTER 18
INFORMATION SYSTEM (IS) SECURITY

1. Purpose. To emphasize general computer and other IS security oversight as delineated by the Department of the Navy, and OPNAV IA Program regulations and established PSAG unique requirements for monitoring of IS vulnerabilities.

2. E-Ring Activities. OPNAV activities located on the Pentagon outermost E-ring shall be aware of the electronic, line of sight, and other perceived threats that may be directed from adjacent locations to the Pentagon Reservation property or from high points in the near vicinity through the outer windows. Occupants of outlying Navy workspaces will also consider the same threat measures before positioning of computer monitors. In an effort to limit the threat risk, office personnel will ensure placement of countermeasures that would limit threat penetrations from outside of the building. To further reduce the threat, OPNAV (DNS-34), OPNAV (DNS-44), and directorate security coordinators will ensure that workstations are aligned as far from windows as feasible and monitors are oriented perpendicular to the windows and outer walls. Cathode-ray tube, CRT, monitors are not authorized in the Pentagon E-ring spaces and all new or replacement monitors in those spaces shall be liquid crystal display or alternative technology to preclude leakage.

3. Command Responsibility and Authority. OPNAV (DNS-4) is designated to establish computer security policy and ensure program effectiveness and compliance with higher directives. Enforcement of IS security matters, administration of IS and security awareness for Navy personnel assigned to OPNAV resides with OPNAV (DNS-44). Physical security of IS is provided in accordance with chapter 11 of this instruction and reference (r). Spaces will be certified by OPNAV (DNS-34) as determined in reference (b) for IS employability and use as part of open storage certification process. Security coordinators designated by each OPNAV directorate will work in conjunction with their directorate ACTR to ensure the directorate maintains IS security compliance. ACTRs will be nominated by directorate and designated by OPNAV (DNS-4) in writing per exhibit 18A of this chapter.

4. User Role and Responsibilities. For OPNAV IS security policy, user's roles and responsibilities are provided in reference (d). Users must be aware of the potential threat at

MAR 23 2009

all times while using IS hardware and software. In addition to specific guidance provided by above referenced documents, users are advised to:

- a. Complete annual IA training and related OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N).
- b. Safeguard information and IS from unauthorized or inadvertent modification, disclosure, destruction, or use.
- c. Protect CUI and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- d. Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- e. Virus check all information, programs, and other files prior to uploading onto any Navy IS resource.
- f. Report all security incidents immediately in accordance with local procedures and security regulations.
- g. Access only that data, control information, software, hardware, and firmware for which users are authorized access and have a "need-to-know," and assume only those roles and privileges for which they are authorized.
- h. Be subject to monitoring, and further understand that there is no individual right to privacy over the data and communications generated through IS use.
- i. Users shall not:
 - (1) Access commercial Web-based e-mail (e.g., HOTMAIL, YAHOO!, AOL, GMail, etc.);
 - (2) Auto-forward official e-mail to a commercial e-mail account;
 - (3) Bypass, strain, or test IA mechanisms (e.g., firewalls, content filters, anti-virus programs, etc.) without coordination and written approval from OPNAV (DNS-44);

MAR 23 2009

(4) Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource;

(5) Relocate or change equipment or the network connectivity of equipment without authorization from OPNAV (DNS-44);

(6) Use personally owned hardware, software, shareware, or public domain software without authorization from OPNAV (DNS-44);

(7) Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of OPNAV (DNS-44);

(8) Participate in or contribute to any activity resulting in a disruption or denial of service;

(9) Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code; and

(10) Use Navy IT resources that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

j. Transfer of data between classified and unclassified systems. Only personnel properly trained and designated, in writing, by OPNAV (DNS-44) are authorized to perform data transfers within OPNAV. Currently, OPNAV (DNS-44) is the only permanently authorized directorate to perform data transfers. Users requesting data transfers between systems must contact OPNAV (DNS-44) to obtain the current data transfer policies.

k. Use screen saver with password if away from system for more than 10 minutes.

l. Use a combination of two uppercase, two lowercase, two numbers and two symbols in your password (nine characters minimum). Administrator/developer/root/super user accounts must contain a 15 character minimum.

m. Be aware of and report indications of virus infections to NMCI, OPNAV (DNS-34), and OPNAV (DNS-44).

MAR 28 2000

5. OPNAV Outlook Web Access (OWA) Requirements. When an OPNAV user requires remote access to Navy IS, that user should be assigned a government laptop which provides dial-up and broadband remote access service. If the user has not been assigned a government laptop or if the laptop connection does not provide sufficient remote access, permission may be granted to access NMCI e-mail using OWA and a non-government computer. The following applies to OPNAV OWA access:

a. OPNAV directorates are responsible for validating each users' OWA requirements. The validation process includes coordination with the directorates respective budget coordinator to purchase the required and appropriate CAC reader.

b. Prospective OWA users will be provided the OPNAV User Responsibilities and Acknowledge and the OPNAV Remote Access Request Memorandums by the command ACTR, who will also direct users to the specific Web site for completing OWA training course "NMCI Outlook Web Access (OWA) Policy Training."

c. Permission to use OWA for remote access to unclassified NMCI e-mail can be granted only after the user's directorate has validated the users requirement and after completion of all required forms and online training.

d. Upon receipt of the completed memorandums and certificate of completion for the online training course, OPNAV (DNS-44) will issue the appropriate middleware for use with the CAC reader. OPNAV (DNS-44) retains all approved requests for OWA access. Annual OWA refresher training is required for all authorized OWA users.

e. The directorate authorizing OWA access is responsible for obtaining CAC readers and establishing a process for issuance of CAC readers to their authorized users. CAC readers will be retrieved from individuals prior to their transfer or when CAC reader use is no longer required. Directorates will confirm and notify OPNAV (DNS-44) when the middleware has been removed from the OWA user's non-DoD computer so the middleware can be returned to inventory or reassigned.

f. All authorized OWA users must comply with all required procedures and computer configuration requirements.

MAR 28 2000

6. Portable Computer Devices Requirements

a. According to Deputy Secretary of Defense Memorandum of 14 July 2000, "there is a need for constant vigilance and strict adherence to established procedures for the protection of official and sensitive department information, particularly classified information. The proliferation of small portable computer devices, with their unprecedented capacity to house vast amount of information, increase not only risk, but also the consequences of an incident involving the loss of even a single computing device." This statement still stands true today. OPNAV personnel must pay close attention to regulations and strictly comply with established procedures for:

- (1) Use and protection of portable computing devices and removable media;
- (2) Cellular phones use and restrictions;
- (3) IT wireless security policy;
- (4) Policy on photography and imaging technology in Pentagon and related NCR facilities; as well as
- (5) Security of Pentagon computer workstations.

b. Further information is provided as follows:

(1) Reference (v) establishes Navy policy on the use of portable storage devices, such as zip drives, recordable CD re-writeable DVD, flash/thumb drives, memory sticks and mini external hard drives, that can be easily attached and removed from NMCI systems without notice.

(a) Use of Universal Serial Bus (USB) portable electronic storage devices on classified and unclassified IS is as follows:

1. Flash Drives, thumb drives and digital camera memory cards are not authorized on any Navy IS;

2. Government owned USB external hard drives are the only USB portable electronic storage devices authorized for utilization on Navy IS. Devices are required to be virus scanned and receive written approval from OPNAV (DNS-44) prior to utilization on any Navy IS; and

MAR 23 2009

3. These devices become permanently classified at the same level of the system unless the device is physically locked to "read only" and when following procedures posted at <https://infosec.navy.mil>.

(b) Non-USB portable electronic storage devices include: DVDs, CDs-Ready Only Memory, and floppy disks. These devices are the only non-USB portable electronic storage devices authorized for use on any Navy Information System. Proper utilization of these devices include:

1. Limited to only those devices required to perform an official DoD, DON or OPNAV operational mission requirement.

2. Personally owned devices are not authorized on any Navy IS.

3. Government procured devices are authorized on Navy IS only after the device has been properly scanned and the authorization request has been received and approved by OPNAV (DNS-44).

4. All portable electronic storage devices will be labeled with overall classification and associated markings using appropriate label.

5. Storage and protection of CUI consisting of personally identifiable data for 500 or more is required in accordance with DoD guidance.

6. Requires proper chain of custody procedures as required by the overall classification of the device.

7. In the event that classified information or CUI contained on a portable electronic storage device is lost, stolen, or misplaced, OPNAV (DNS-34) and OPNAV (DNS-44) must be notified immediately.

8. Electronic portable storage devices impacted by an ES must be surrendered to OPNAV (DNS-44) and/or NMCI as directed for ES cleanup and mitigation.

(c) Thumb drives; flash drives; flash cards; cameras; cell phones; smart phones; music players; and all other portable electronic storage devices not authorized above are not authorized for use on any Navy IS at this time.

MAR 23 2009

(2) Destruction of all portable storage devices, hard drives, and classified software will be in accordance with procedures outlined in chapter 12 of this instruction and the ACTR designation letter per exhibit 18A of this chapter. Hard drive destruction will be coordinated with the security coordinator and documented on OPNAV 5239/15 Classified Hard Drive Destruction Log.

(3) Cell phone and other wireless device vulnerabilities:

(a) Cell phones (including Personal Digital Assistant (PDA)s and blackberries) will be surrendered before entering SCI facilities and spaces where either classified communications or electronic information processing is taking place. Personnel must also be aware that some facilities do not have the capability to hold phones, thus leaving the phone in the car is a better solution. Cell phones (including PDAs and blackberries) may enter into other open storage spaces but must be turned off and may not be used without proper clearance from space custodian or security coordinators. All personnel must be aware of inherent cell phone vulnerabilities as follows:

1. Conversations could possibly be monitored while using the phone;

2. The cell phone could possibly act as a microphone to transmit conversations in the vicinity of the cell phone even though the phone is inactive;

3. The phone number could be "cloned" or used by others to make calls that are charged to the user's account.

(b) Other wireless devices, such as PDA, personal electronic devices, blackberries, or any other with infrared capability, must be turned off and/or disconnected from their battery source upon entering spaces where classified communications, including VTC or electronic information processing, are taking place. Information protection begins with each OPNAV Sailor, civilian and contractor employees, and all must be mindful of both the threat and systems vulnerabilities. See the command security manager, OPNAV (DNS-44) and security coordinators for posting of requirements and availability of the latest PSAG wireless communications reference documents.

MAR 28 2000

EXHIBIT 18A

S-A-M-P-L-E

5510
DNS-4
<date>

From: Chief of Naval Operations Command Information Officer
(DNS-4)

To: Individual Appointed (full name, office code,
location and telephone number)

Via: Directorate Head

Subj: DESIGNATION AS NAVY AND MARINE CORPS INTRANET (NMCI)
ASSISTANT CONTRACT TECHNICAL REPRESENTATIVE (ACTR)

Ref: (a) Executive Order 12958, as amended 25 March 2003
(b) SECNAV M-5510.36, Department of the Navy
Information Security Program (ISP) Manual
(c) SECNAV M-5510.30, Department of the Navy
Personnel Security Program (PSP) Manual
(d) SECNAVINST 5239.3A, Department of the Navy
Information Assurance (IA) Policy
(e) OPNAVINST 5530.14E, Navy Physical Security and
Law Enforcement Program
(f) USSAN 1-70, United States National Security
Authority for NATO (USSAN) Instruction (Industrial
Security) (NOTAL)
(g) DoD Directive 5210.2, Access to and Dissemination of
Restricted Data, 12 Jan 1978
(h) CNO ltr 5510 N09N2/8U223000 of 7 Jan 2008, Subj:
Updated Policy for "Declassify On" Markings (NOTAL)
(i) OPNAVINST 5513.1F, Department of the Navy Security
Classification Guides
(j) DoD Manual 5220.22-M, National Industrial Security
Program Operating Manual, 28 Feb 2006
(k) SECNAVINST 5720.42F, Department of Navy Freedom of
Information Act Program
(l) OPNAVINST 5511.35L, Safeguarding Nuclear Command and
Control Extremely Sensitive Information
(m) SECNAVINST S5460.3F, Management, Administration,
Support, and Oversight of Special Access Programs
Within the Department of the Navy (NOTAL)
(n) NAVSEAINST 5511.32C, Safeguarding of Naval Nuclear
Propulsion Information (NOTAL)

MAR 23 2009

- (o) SECNAVINST 5720.44B, Department of the Navy Public Affairs Policy and Regulations
- (p) SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
- (q) Naval Information Assurance Publication, IA Pub-5239 -22, Oct 2003
- (r) SECNAVINST S8126.1, Naval Nuclear Weapons Security Policy (NOTAL)
- (s) DoD Instruction 5200.33, Defense Courier Operations, 19 May 07
- (t) OPNAVINST C5510.159, Guidelines Applicable to Communist Nationals Entering the United States as Non-Immigrant Aliens (NOTAL)

1. You are hereby appointed as an Assistant Contract Technical Representative (ACTR) for all NMCI services required in support of your assigned Directorate. Your period of appointment shall be a minimum of one year from the date of this letter. In the performance of your ACTR duties, you will be required to become familiar with the guidance in references (a) thru (k). You will represent your Directorate, and coordinate with the OPNAV NMCI Contract Technical Representative (CTR) (OPNAV (DNS-43)). You are also required to coordinate your ACTR duties with your Directorate's Command Security Coordinator to ensure full compliance with current security regulations in accordance with reference (d).

2. Your duties and responsibilities as an NMCI ACTR include:

a. Maintaining Directorate's accounts in the following NMCI related on-line tools: Service Request Electronic Form (SReForm); Navy Enterprise Tool (NET); and Information Strike Force (ISF) Tools.

b. Conducting in-processing for all new Directorate personnel to include:

- (1) Verifying security clearance with your Directorate's Command Security Coordinator;
- (2) Providing brief on their security responsibilities;
- (3) Determining and ordering NMCI service requirements;

MAR 23 2003

(4) Transferring existing or creating new NMCI user accounts; and

(5) Ensuring OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N) forms are completed and routed to the Command Information Assurance Manager, OPNAV (DNS-44).

c. Acting as your Directorate's focal point for all NMCI requirements to include:

(1) Assisting Directorate users with submitting trouble tickets;

(2) Preparing Move-Add-Change (MAC) requests; and

(3) Maintaining the NET database for accurate accounting and billing for all Directorate user accounts and NMCI delivered services and assets.

d. Maintaining up-to-date familiarity with NMCI Contract Line Item Numbers (CLINs). They are used in the ordering and accounting of NMCI services and change routinely.

e. Conducting monthly survey of all NMCI services being provided to the Directorate to identify:

(1) New service requirements. Coordinate ordering, funding and delivery with the Directorate and the OPNAV CTR. Verify actual date of full delivery of all NMCI services to provide full invoice accounting to the OPNAV CTR;

(2) Services due for technical refresh. Coordinate replacement schedule with the Directorate and the OPNAV CTR; and

(3) Services no longer required by the Directorate. Coordinate termination and equipment turn-in with the Directorate personnel and the OPNAV CTR. If the services being terminated involve classified material (including classified computers, hard drives, storage devices, etc.), the ACTR shall coordinate turn-in with the Directorate's Command Security Coordinator and the OPNAV CTR. All classified material handling and destruction requirements shall be in accordance with Chapter 12 of reference (d).

MAR 28 2009

f. Supporting the Directorate Command Security Coordinator and the Command Information Assurance Manager (IAM), as required.

g. Assisting Directorate personnel with contacting the NMCI Helpdesk and escalating trouble tickets that are not being resolved in a timely manner. If additional escalation is required to resolve a trouble ticket, the ACTR shall coordinate with the OPNAV CTR.

h. Coordinating any Directorate personnel moves (internal or external to their current office) with the OPNAV CTR prior to actual move to properly plan, document, and ensuring minimal service interruption to the user. Coordination includes but is not limited to:

(1) Providing move details and timelines to the OPNAV CTR;

(2) Submitting requirements for all Pentagon and NCR infrastructure changes; and

(3) Submitting updates to the NET tool and providing MAC for all NMCI hardware asset physical moves and/or NMCI active directory changes.

i. De-activating or transferring all NMCI user accounts upon their departure from the Directorate and/or the command. Submit updates to the NET tool, and provide MAC requests for all NMCI hardware asset physical moves and active directory changes.

j. Ordering new NMCI services and conducting the periodic technical refresh of existing NMCI services. ACTR duties include:

(1) Ensuring the following information is correct in the NET tool: all NMCI SIPRNET and NIPRNET requirements; personal data for each individual user (profile and account information); and asset information, including asset tag number and location.

(2) Ensuring all software applications required for each user are identified correctly and associated with the correct user and asset in the NET tool.

MAR 23 2009

(3) Prior to delivery, coordinating NMCI delivery of any new services, equipment, or software applications with the appropriate Directorate office personnel and the OPNAV CTR.

(4) For SIPRNET desktop computers, coordinating receipt of all classified internal hard drives with the Directorate's Command Security Coordinator. Ensure all "chain of custody" paperwork is completed to transfer classified material to the end user.

3. Proper handling, transfer, and/or destruction of classified NMCI materials in accordance with current security regulations, protocols and procedures are integral to adequately perform the ACTR function. Classified NMCI materials includes all classified hard drives/desktop and laptop computers/storage devices or media. To prevent security incidents, ACTRs will ensure compliance with all requirements outlined in references (a) thru (k) and the following:

a. Contractor personnel, to include NMCI support personnel, are not authorized to hand carry any classified NMCI material out of designated Security Serviced Activity spaces without prior arrangements and approval of the OPNAV Command Security Manager (DNS-34) via their Directorate's Command Security Coordinator in accordance with reference (d).

b. Military/government civilian personnel are not authorized to remove any classified NMCI material from their designated office or working area except in the performance of their official duties in accordance with reference (d).

c. Under no circumstances can any personnel remove any classified NMCI material from designated work areas to use during off duty hours, or for any other purpose involving personal convenience, without specific approval of the OPNAV Command Security Manager (DNS-34) via their Directorate's Command Security Coordinator in accordance with reference (d).

d. The ACTR shall coordinate all service termination and turn-in of classified NMCI material, in advance, with the Directorate's Command Security Coordinator and the OPNAV CTR. Ensure all classified material handling and destruction complies with Chapter 12 of reference (d).

(1) For classified desktops and laptops, remove classified hard drives and all classification stickers. When

MAR 23 2009

removing the hard disk drive from the chassis or cabinet, also remove any steel shielding material or mounting brackets which may interfere with magnetic fields. Maintain custody of desktops and laptops that have had their hard drives and classification stickers removed within the Directorate secure spaces until proper custody transfer is coordinated by the ACTR with the Directorate's Command Security Coordinator and the OPNAV CTR.

(2) Classified hard drives shall be placed in burn bags that contain no other material. The bags must be clearly labeled as containing hard drives. No more than five hard drives shall be allowed per bag.

(3) Classified media, such as CDs, cassettes, or VCR tapes may be mixed in burn bags containing other classified papers and materials.

(4) All burn bags must be protected and stored within the Directorate secure spaces and out of view from the office entrance doors at all times until it is time to deliver to the Pentagon Remote Delivery Facility (RDF) for destruction.

(5) In coordination with the Directorate's Command Security Coordinator, record the destruction of all burn bags containing NMCI related classified material at the Pentagon Remote Delivery Facility (RDF), and provide copies to the OPNAV CTR. Components are not considered destroyed until a signed notice of destruction is received from the approved destruction organization.

4. Training is essential for successful performance of the ACTR duties. ACTRs must complete the following training within 90 days of designation. Failure to complete this training will result in this ACTR designation and all authority it grants being revoked until such time as the training is fully completed.

a. Complete the computer-based training modules on the CTR training website: <https://www.homeport.navy.mil/training/ctr/>

b. Attend an ACTR training session held by the OPNAV CTR. These sessions are conducted on a quarterly and by request basis.

MAR 28 2000

c. Complete the annual Navy NETWARCOM directed Information Assurance (IA) refresher training on Navy Knowledge Online (NKO).

5. Violations of the referenced instructions and this designation letter.

a. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of the referenced instructions and this designation letter.

b. Civilian employees are subject to criminal penalties under applicable Federal Statutes, a well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of the referenced instructions and this designation letter.

6. Your signature below acknowledges your responsibility as an ACTR for your Directorate. Your support and professionalism are necessary for success of your Directorate's and OPNAV Staff's mission. While each person in your Directorate are individually responsible for their own NMCI accounts, equipment, and actions while using NMCI, your integral involvement in the NMCI ACTR program ensures the continued availability and security of NMCI services for your Directorate, OPNAV and the Navy. You will be notified of any change in this appointment.

Designee's Signature/Date: _____/_____

OPNAV CIO (DNS-4) Signature/Date: _____/_____

Copy to:

Personnel File

OPNAV Command Security Manager (DNS-34)

OPNAV Command NMCI Contract Technical Representative (DNS-43)

MAR 28 2000

CHAPTER 19
EMERGENCY PROCEDURES AND NOTIFICATIONS

1. Purpose. To establish policy and standardize procedures for emergency and notification requirements in Navy spaces on the Pentagon Reservation. For Pentagon and FOB#2 occupants, PFPA will provide instructions over the "Big Voice" Public Announcement (PA) System and CENS during crises. For those employees housed in other building in the NCR, the respective buildings manager will outline building unique requirements in their emergency action procedures.

2. Procedures

a. Duty to report - Occupants of facilities on the Pentagon Reservation shall promptly report all crimes and suspicious circumstances occurring on the Pentagon Reservation to PFPA, (703) 697-5555, and to OPNAV (DNS-34) at (703) 697-3454. PFPA communications center shall dispatch a police officer to the scene of the offense and/or incident to conduct an investigation.

b. Fire or smoke - Any person who observes fire or smoke should activate the nearest alarm box. If the person smells something burning, he or she shall notify PFPA at (703) 695-5555, and provide the room number or location of the possible fire.

c. Building Evacuations - During emergencies and when directed by either PFPA, building manager or building emergency occupant official, personnel could be directed to:

(1) Shelter in Place - meaning it is safer inside;

(2) Internal Relocation - moving to another place in the building is safer than going outside; and

(3) Evacuation - stay calm, do not panic and follow instructions through the designated exit per emergency implementation plan to specific assembly areas.

d. Medical Emergencies - Notify PFPA at (703) 697-5555. PFPA will contact the appropriate medical emergency service.

MAR 23 2009

e. Suspicious Persons and/or Packages - Any person discovering a suspicious package or observing a suspicious person shall notify PFPA at (703) 697-5555. Do not touch or move any suspicious articles.

f. Nuisance Calls, Persons, or Letters - Unsolicited contacts may be in person, in writing, or by telephone. Information may be received about individuals or organizations that may pose a threat to the safety and security of Government officials. Prompt notification should be given to PFPA on all threats. Contacts that do not contain a direct threat to do harm but indicate intent to embarrass or harass should not be ignored. Chronic letter writers and multiple telephone calls from an individual generally create more of a nuisance than a threat. However, each occurrence should be monitored closely to determine any attitude changes in individuals.

g. Bomb Threats - Any person receiving a bomb threat should attempt to record the following and immediately telephone PFPA at (703) 697-5555:

- (1) Exact words of caller.
- (2) Time the device is to explode.
- (3) Location of the device.
- (4) Time and date of call.
- (5) Name of caller.
- (6) Sex of caller.
- (7) Accents or dialects.
- (8) Age (i.e., young or old).
- (9) Background noises heard telephone.

h. Hostage or Terrorist Incident - Notify PFPA at (703) 697-5555.

i. FPCON - Refer to chapter 17 of this instruction.

MAR 23 2009

3. Notifications

a. OPNAV (DNS-34) receives from PFPA, via e-mail, phone or conferencing switch, emergency alert information on incidents occurring on the Pentagon Reservation. Based on the actual threat received, OPNAV (DNS-34) will notify command security coordinators by the following means:

(1) Telephonic notification to all principal officials, security coordinators and Navy Command Center.

(2) Flash e-mail message to all OPNAV security serviced activities' computer account holders.

(3) "BIG VOICE" announcement throughout Navy Pentagon spaces via coordination with PFPA if telephone and computer system are down.

b. OPNAV (DNS-34) will pass on available details from PFPA or other sources without jeopardizing either time or situational integrity. Due to the large number of personnel to notify, the OPNAV (DNS-34) will not answer phone questions during time of crises. Incoming calls must be held to minimum to ensure passing of critical information during crises situations.

c. At times of emergency, follow directions to egress exit from the buildings as identified in emergency response implementation plans, remain in place or relocate internally. Ensure that adjacent offices receive notification that personnel must immediately leave, stay put or relocate in the building. Special consideration must be taken to ensure safety for physically disabled personnel and emergency procedures will specify safe provisions for immobile individuals.

MAR 23 2009

APPENDIX AOPNAV SECURITY SERVICED ACTIVITIES' UICs

The following UICs reported under one UIC (65146) for personnel security clearances in JPAS under SMO 000114:

<u>UIC</u>	<u>NAME</u>	<u>OASIS ENTRY</u>
00011	Office of the Chief of Naval Operations	By Serviced Activity*
00012	Assistant for Administration, Under Secretary of the Navy	AAUSN
00013	Navy Judge Advocate General	JAG
00166	Naval Air Facility, Andrews AFB (PNT Only)	N095
30320	Department of the Navy Office of Process, Technology and Information	OPTI
30346	Board for Corrections of Naval Records	BCNR
30571	Office of General Counsel	OGC
31572	Chief of Naval Personnel DET, Washington	N1
31698	Office of the Secretary of the Navy	SECNAV
31699	Office of Under Secretary of the Navy	AAUSN
31701	Maritime Domain Awareness	SECNAV
31702	Office of the Assistant Secretary of the Navy, Financial Management Comptroller	FMC
31703	Deputy Under Secretary of the Navy, Office Integration Group	OIG

MAR 23 2009

31705	Chief of Information Office	CHINFO
31706	Office of Program and Process Assessment	OPPA
31707	Navy Department Board of Decorations and Medals (SECNAV awards that merged with DNS-35/only 2 billets under this UIC)	SECNAV
31863	Naval Audit Service	NAVAUD
31975	Chief Information Officer	CIO
32748	Secretary of the Navy, Council of Review Boards	SECNAV CORB
32790	Secretary of the Navy, Reserve Navy Activity	By Serviced Activity*
32791	Chief of Naval Operations Reserve Pay (PNT Only)	By Serviced Activity*
3344B	Bureau of Naval Personnel (Annex only)	N1
3495B	Bureau of Naval Personnel (Pers-6 Washington Liaison DET at Annex)	N1
35058	Department of the Navy Staff Offices	By Serviced Activity*
32039	COMNAVAIRFORCE DET Reserve Pay Navy	N88
3833A	Bureau of Naval Personnel (Annex Only)	N12/N13
39480	Navy Inspector Generals Office	NAVINSGEN
41421	Office of the Deputy Comptroller	FMC
42217	Office of the Assistant Secretary of the Navy, Manpower and Reserve Affairs	ASNMRA

MAR 23 2009

42485	Assistant for Administration Under Secretary of the Navy Immediate Office	AAUSN
43023	OPNAV Navy Command Center	N3N5
43116	ASNIE Guam Program Office	ASNIE
43440	Bureau of Naval Personnel (2 billets Annex)	N1
44690	Civil Law Support Activity	JAG
44802	ONI/N2 Check-in w/CNO (SSO),	
4577A	Chief of Naval Operations and Bureau of Naval Personnel (has N1 billet and an N8 billet)	By Serviced Activity*
45997	Bureau of Naval Operations (Annex/PNT)	N1
46699	Chief of Naval Education and Training (Personnel permanently assigned to Annex/PNT)	N1
47039	Office of the Chief of Naval Operations	By Serviced Activity*
47218	Dep Under Secretary of the Navy	ONI/N2 Reassignments
47326	Naval Inspector General	NAVINGEN
47402	OPNAV JMCIS/GCCS	N3N5
47454	Commander Naval Reserve Force Staff DET (N095 PNT Employees Only)	N095
47692	Navy Industrial Management Program (includes BRAC Project Office)	ASNIE
48142	Assistant Secretary of the Navy Research, Development and Acquisition	ASNRDA

MAR 28 2000

48142	C4I Chief of Information Office	CIO
48143	Assistant Secretary of the Navy Installations and Environment	ASNIE
48144	Office of the Under Secretary of the Navy Support Center (TQM)	AAUSN
48145	Director, Small and Disadvantaged Business Utilization	AAUSN
48146	Assistant Deputy Under Secretary of the Navy, Safety and Survivability	AAUSN
48766	Naval Financial Management Career Center, NAS Pensacola	FMC
48858	SPEC BDS COMMITS Naval Inspector General Support	NAVINSGEN
49440	NAVSPECWARCOM	
49933	Human Resources Field Support Office (S/HHRO Employees)	AAUSN
49943	STU Legislative Affairs Fellows Program	OLA
62695	Naval Audit Service Headquarters	NAVAUD
62980	Commander Naval Reserve Force Staff DET	By Serviced Activity*
63423	OPNAV DET Site "R"	N3N5
63959	Quarters Chief of Naval Operations (For military personnel assigned to Flag Quarters in National Capital Region/PQMESS)	By Serviced Activity*
64243	SPEC BDS COMMITS ACT	NAVINSGEN

MAR 28 2000

65116	Navy-Marine Corps Appellate Review Activity (NAMARA)	JAG
65146	OPNAV Support Activity	By Serviced Activity*
66123	Navy Department of Legislative Affairs	OLA
66760	Navy Public Affairs Office Navy Department Staff Offices	CHINFO
68027	Commerce Department (NOAA) (formerly N096 & N7C Naval Observatory)	N84
68499	Navy Council of Review Boards	SECNAV CORB
68864	Naval Center for Cost Analysis	FMC
68910	Legal Services Support Group	OGC
83852	Senior Executive Office for Manpower Personnel (4 billets)	N095
68323	Navy Legal Services Command - JAG Security Coordinator is the security manager for this command. Personnel assigned to this command should check in with JAG not OPNAV Security	

*Listing of valid OPNAV Codes for OASIS Entry

N00	N3N5	N87	NAVAUD
N00K	N4	N88	NAVINGEN
N09	N6	N89	OGC
N09X	N61	SECNAV	OLA
N091	N6F	AAUSN	OPPA
N093	N8	ASNIE	OPTI
N095	N8F	ASNMRA	SAT
N097	N80	ASNRDA	SECNAV CORB
DNS	N81	BCNR	
N1	N84	CHINFO	
N10	N85	FMC	
N12N13	N86	JAG	